VNIVERSITAT
DE VALÈNCIA

Characters, Fields of Values and Conjugacy Classes in Finite Groups

Memòria per optar al grau de
Doctor en Matemàtiques
realitzada per
Joan Francesc Tent Jorques
dirigida per
Gabriel Navarro Ortega

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

D. Gabriel Navarro Ortega, Catedràtic d'Universitat del Departament d'Àlgebra de la Universitat de València,

CERTIFICA:

Que la present Memòria, titulada "Characters, Fields of Values and Conjugacy Classes in Finite Groups", ha estat realitzada sota la meva direcció per D. Joan Francesc Tent Jorques per optar al grau de Doctor en Matemàtiques, amb menció "Doctor Europeus".

Així ho faig constar en compliment de la normativa vigent.

Burjassot, 14 de març de 2012

Signat: Gabriel Navarro Ortega

A la meva família

Contents

Agraïments

Vull en primer lloc donar les gràcies al meu director de tesi, Gabriel Navarro, per la confiança dipositada en mi i per la seva ajuda i suport en la realització d'aquest treball. Sense ell aquesta tesi no hauria sigut possible.

També vull donar les gràcies a Alex Moretó per moltes converses sobre matemàtiques, i a Lucia Sanus per totes les ocasions en què m'ha ajudat.

A la resta del departament d'Àlgebra de la Universitat de València, per oferir un gran entorn per poder realitzar una tesi doctoral.

A Marty Isaacs, Josu Sangroniz, Silvio Dolfi i Geoff Robinson per oferir-me l'oportunitat de realitzar estàncies en altres departaments i per tota l'ajuda que m'han proporcionat en la meva investigació.

Agraesc el programa de beques FPU del Ministeri d'Educació i els distintints projectes d'investigació del Ministeri de Ciència i Innovació en què he participat pel finançament del projecte de tesi doctoral.

I molt especialment vull donar les gràcies a la meva família i els meus amics per tot el suport i l'encoratjament que m'han donat.

Ackowledgements

First, I want to express my gratitude to my advisor, Gabriel Navarro, for his confidence, help and support. Without him, this work would not have been possible.

I also want to thank Alex Moretó for many helpful conversations about mathematics, and Lucia Sanus for being so helpful in many occasions.

I thank the Department of Algebra at the University of València, for providing a great environment to do research.

I want to thank Marty Isaacs, Josu Sangroniz, Silvio Dolfi and Geoff Robinson for giving me an opportunity to visit their universities and for all the help in my research.

I appreciate the finantial support provided by the grant FPU (Ministerio de Educación, Spain) and by the research projects in which I took part (Ministerio de Ciencia e Innovación, Spain).

Finally, very special thanks to my family and friends for their constant support and encouragement.

Resumen

Introducción

Una cuestión fundamental en la Teoría de Caracteres de Grupos Finitos consiste en estudiar la información sobre la estructura de un grupo finito que está contenida en su tabla de caracteres irreducibles. Las entradas que aparecen en la tabla de caracteres pueden estudiarse desde distintos puntos de vista, los cuales están a menudo estrechamente relacionados entre sí.

Como ilustran los resultados en la literatura especializada, el conjunto de los grados de los caracteres irreducibles de un grupo finito (primera columna de la tabla de caracteres del grupo), contiene información no trivial sobre la estructura del grupo. El teorema de Ito-Michler (si un primo p no divide los grados de los caracteres irreducibles de G, entonces G tiene un p-subgrupo de Sylow normal), es un ejemplo muy destacable de este tipo de resultados, en los cuales consideraciones de tipo aritmético son a menudo relevantes. Otro foco de interés en investigaciones recientes en Teoría de Caracteres ha sido el conjunto de ceros en la tabla de caracteres de un grupo, así como otros conjuntos relacionados, comprobándose que los ceros de la tabla de caracteres también reflejan aspectos de la estructura del grupo correspondiente.

El punto de vista que nosotros adoptamos en esta memoria, el cual también ha sido explorado en la literatura previamente, es el análisis de cuerpos de valores de caracteres ordinarios y su relación con ciertos invariantes del grupo. En este contexto, las cuestiones sobre racionalidad en grupos finitos se hallan entre las más interesantes y, como veremos, algunos de nuestros resultados más importantes tratan problemas que involucran caracteres que toman valores en el cuerpo de los racionales (**caracteres racionales**) y clases de conjugación que contienen elementos racionales (**clases racionales**) en grupos finitos.

Es bien conocido que los caracteres de un grupo finito toman valores en extensiones ciclotómicas del cuerpo de los números racionales, de modo que no resulta sorprendente que la Teoría de Galois juegue un papel importante en el estudio de los cuerpos de valores de grupos finitos, y en nuestro trabajo en particular. A modo de introducción, y dada su relevancia en la obtención de nuestros resultados, a continuación describimos cómo algunas de las técnicas de la Teoría de Galois pueden aplicarse en el análisis de cuerpos de valores de grupos finitos. Estos resultados preliminares pueden encontrarse en el Capítulo 1, donde además se presentan algunos resultados básicos de la Teoría de Caracteres de Grupos Finitos que son necesarios a lo largo del trabajo.

Sea G un grupo finito. El conjunto de caracteres irreducibles complejos de G se denota por $\mathrm{Irr}(G)$, y el conjunto de clases de conjugación de G es designado por $\mathrm{Cl}(G)$. Como es

usual, si g es un elemento de G, escribimos $\mathrm{Cl}_G(g)$ para la clase de conjugación de g en G. No es difícil probar que todo carácter irreducible de G se puede ver como el carácter de una representación irreducible $\mathcal{X}$ de G, sobre un cuerpo E que es una extensión finita de Galois sobre el cuerpo de los racionales $\mathbb{Q}$. Además, se puede suponer que E contiene una raíz n-ésima primitiva compleja de la unidad, donde n es un múltiplo del exponente de G. Esta observación implica que el grupo de Galois $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ actúa de manera natural sobre el conjunto de caracteres irreducibles de G. Más concretamente, sean $\chi \in \mathrm{Irr}(G)$ y $\sigma \in \mathcal{G}_n$; definimos

$$\chi^\sigma(g) = \chi(g)^\sigma$$

para todo $g \in G$. Se puede comprobar que efectivamente $\chi^\sigma \in \mathrm{Irr}(G)$, y en particular se deduce que $\mathcal{G}_n$ actúa sobre los caracteres no necesariamente irreducibles de G.

Siguiendo con la misma notación, el grupo de Galois $\mathcal{G}_n$ también actúa de manera natural sobre el conjunto de las clases de conjugación $\mathrm{Cl}(G)$ de G. Por teoría elemental de cuerpos, un automorfismo $\sigma \in \mathcal{G}_n$ está unívocamente determinado por un número entero t, que es coprimo con n y único módulo n, tal que t satisface la ecuación $\xi^\sigma = \xi^t$ para cualquier raíz n-ésima primitiva de la unidad $\xi \in \mathbb{C}$. Sea g un elemento de G. Entonces escribimos

$$\mathrm{Cl}_G(g)^\sigma = \mathrm{Cl}_G(g^t)\,,$$

y se puede ver fácilmente que esta expresión define una acción de $\mathcal{G}_n$ sobre las clases de conjugación de G.

Las acciones de $\mathcal{G}_n$ sobre $\mathrm{Irr}(G)$ y sobre $\mathrm{Cl}(G)$ no son isomorfas como permutaciones en general, aunque están estrechamente relacionadas. Por el Lema de las Permutaciones de Brauer, un automorfismo cualquiera $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ fija el mismo número de caracteres irreducibles de G que de clases de conjugación de G. En particular, en un grupo finito cualquiera, el número de caracteres que toman solo valores reales (**caracteres reales**) coincide con el número de clases de conjugación en las que todos los caracteres de G toman valores reales (**clases reales**), ya que los caracteres y las clases reales son precisamente aquellos fijados por la conjugación compleja.

Sea $\chi \in \mathrm{Irr}(G)$. El **cuerpo de valores** de χ en G es, por definición, el menor cuerpo que contiene todos los valores que toma el carácter χ en el grupo G, es decir

$$\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g) \mid g \in G)\,.$$

De modo similar, si $g \in G$, el **cuerpo de valores** de g en G se define como

$$\mathbb{Q}(g) = \mathbb{Q}(\chi(g) \mid \chi \in \mathrm{Irr}(G))\,,$$

es decir, es el menor cuerpo que contiene los valores que los caracteres de G toman en g. A menudo escribimos $\mathbb{Q}(g) = \mathbb{Q}(C)$, donde C es la clase de conjugación de g en G.

Es una consecuencia inmediata de la definición de cuerpo de valores de caracteres y de clases, que el estabilizador de un carácter $\chi \in \mathrm{Irr}(G)$ en la acción natural de $\mathcal{G}_n$ es precisamente

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(\chi)),$$

mientras que el estabilizador de una clase de conjugación $C \in \mathrm{Cl}(G)$ es

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(C)).$$

En particular un carácter $\chi \in \mathrm{Irr}(G)$ es racional si y solo si χ es $\mathcal{G}_n$-invariante, y lo mismo ocurre para las clases de conjugación $C \in \mathrm{Cl}(G)$.

Racionalidad y 2-subgrupos de Sylow

Supongamos que n es un múltiplo del exponente de un grupo G. Las acciones del grupo de Galois $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ sobre los caracteres irreducibles de G y sobre el conjunto de las clases de conjugación G no son isomorfas en general, como hemos indicado antes. Los grupos de menor orden en los que las acciones no son isomorfas tienen tamaño 2^5. Observemos que por los agumentos expuestos en la sección anterior, cuando estas dos acciones son isomorfas, existe una biyección entre las clases de conjugación y los caracteres irreducibles de G que preserva los cuerpos de valores. En particular, en este caso tenemos que el número de clases de conjugación racionales de G es igual al número de caracteres irreducibles racionales de G.

Es importante notar que un grupo G puede tener el mismo número de clases racionales que de caracteres racionales, y sin embargo las acciones de $\mathcal{G}_n$ sobre $\mathrm{Irr}(G)$ y sobre $\mathrm{Cl}(G)$ no ser isomorfas, como lo demuestran ciertos grupos de orden impar, por ejemplo.

Una consecuencia del resultado principal de [2] es que un grupo G tiene el mismo número de clases racionales que de caracteres irreducibles racionales, si los subgrupos de Sylow de G son abelianos, ya que bajo estas condiciones las acciones de $\mathcal{G}_n$ sobre $\mathrm{Irr}(G)$ y sobre $\mathrm{Cl}(G)$ son isomorfas. Otra condición suficiente para obtener la igualdad entre el número de clases de conjugación racionales y el número de caracteres irreducibles racionales de un grupo finito se puede encontrar en [31]: la igualdad es cierta si cualquiera de estos números es igual a 2.

En el Capítulo 2 de esta memoria, contamos las clases racionales y los caracteres racionales de grupos que tienen un 2-subgrupo de Sylow cíclico, y obtenemos el siguiente resultado, que es el teorema principal del capítulo.

Teorema A. *Supongamos que G tiene un 2-subgrupo de Sylow P cíclico. Entonces G tiene el mismo número de clases racionales que de caracteres irreducibles racionales.*

Desafortunadamente, no parece que el Teorema A se pueda generalizar para obtener otros resultados del mismo tipo. De hecho, si cambiamos en el enunciado la condición de que P sea cíclico por $P = C_2 \times C_2$, donde C_2 es el grupo cíclico de orden 2, entonces el Teorema A es falso, incluso si suponemos que G tiene un 2-complemento normal; por ejemplo, existe un grupo de orden $2^2 \cdot 3^4 \cdot 7$ que tiene un 2-subgrupo de Sylow elemental abeliano, un 2-complemento normal y un número de clases racionales distinto al número de caracteres racionales irreducibles.

La demostración del Teorema A no es en absoluto elemental, a pesar de que las hipótesis pueden parecer fuertes. Para obtener el resultado, es necessario usar la π-teoría de Isaacs, la correspondencia de Glauberman-Isaacs y algunos de los argumentos del artículo sobre caracteres cuadráticos en grupos de orden impar [28], entre otros. Los métodos utilizados en el Capítulo 2 son presentados con la suficiente generalidad para que puedan aplicarse en otros puntos del trabajo (especialmente en el Capítulo 5), y permiten también analizar bajo qué condiciones grupos con un p-subgrupo de Sylow normal tienen el mismo número de clases racionales que de caracteres irreducibles racionales. El siguiente resultado también aparece en el Capítulo 2 de la tesis.

Teorema. *Supongamos que $G = PQ$, donde $P \lhd G$ es un p-subgrupo de Sylow de G, para p un primo impar, y Q es un 2-grupo abeliano, diédrico, semidiédrico o cuaternio generalizado. Entonces G tiene el mismo número de clases racionales que de caracteres irreducibles racionales.*

La demostración del teorema anterior depende, además de los resultados previos usados para probar el Teorema A, de la existencia de una correspondencia natural entre las clases de conjugación racionales y los caracteres irreducibles racionales de un 2-grupo diédrico, semidiédrico o cuaternio generalizado.

Los resultados nuevos presentados en esta sección son trabajo conjunto del autor y G. Navarro, y han sido publicados en [30].

2-Longitud y caracteres racionales de grado impar

Es un hecho bien conocido que un grupo finito G tiene orden impar si y solo si G tiene un único carácter irreducible racional. Un refinamiento de este resultado fue conjeturado por R. Gow, quien predijo que todo grupo finito de orden par tiene un carácter irreducible racional no trivial de grado impar.

Recientemente, G. Navarro y P. H. Tiep demostraron que la conjetura de R. Gow es cierta en [31]. Para probar la conjetura, los autores introdujeron nuevas técnicas de extensión de caracteres racionales, que permitieron demostrar una versión más fuerte del resultado para grupos resolubles. Más concretamente, G. Navarro i P. H. Tiep demostraron que si G es un grupo resoluble de orden par, entonces la 2-longitud de G es menor que el número de caracteres irreducibles racionales de G de grado impar.

Nuestro principal objetivo en el Capítulo 3 es obtener una mejora significativa del resultado de G. Navarro y P. H. Tiep que acabamos de mencionar. Podemos demostrar que existe una cota superior logarítmica para la 2-longitud de un grupo resoluble G, en función del número de caracteres irreducibles racionales de grado impar de G.

Teorema B. *Sea G un grupo resoluble y supongamos que la 2-longitud de G es $l \in \mathbb{N}$. Entonces G tiene al menos 2^l caracteres racionales de grado impar.*

Entre les implicaciones de este resultado, encontramos una nueva relación local/global, tal vez inesperada, que no involucra caracteres en el enunciado. Como es habitual, denotamos por $\Phi(P)$ al subgrupo de Frattini de un grupo P.

Corolario. *Sea P un 2-subgrupo de Sylow de G. Entonces el número de órbitas de la acción del normalizador $\mathbf{N}_G(P)$ por conjugación sobre $P/\Phi(P)$ admite una cota inferior logarítmica en función de la 2-longitud de G.*

Veamos ahora otras aplicaciones del Teorema B. Es una consecuencia inmediata de un teorema de J. Thompson (ver IX.8.6 de [12]) que un grupo resoluble con únicamente dos clases de conjugación racionales tiene 2-longitud 1. Recientemente, M. Isaacs y G. Navarro probaron en [18] que la misma conclusión es cierta para un grupo resoluble G que tiene a lo sumo tres clases de conjugación de elementos racionales. Como los autores de [18] muestran, este resultado puede deducirse a partir del Teorema B.

Es natural preguntarse si la cota que el Teorema B proporciona es de hecho una cota óptima. En el Capítulo 3 construimos una sucesión de grupos resolubles

$$G_1, G_2, \ldots, G_l, \ldots$$

tal que G_l tiene 2-longitud l y exactamente 2^l caracteres irreducibles racionales de grado impar, de modo que la cota del Teorema B no se puede mejorar.

Finalmente, el Teorema B admite la siguiente generalización para números primos arbitrarios p y grupos p-resolubles. En la demostración de este resultado más general usamos nuevamente la teoría de los caracteres B_p de Isaacs. Igual que antes, si n es un entero cualquiera, entonces $\mathbb{Q}_n$ es la n-ésima extensión ciclotómica sobre $\mathbb{Q}$.

Teorema. *Sea G un grupo p-resoluble, donde p es un primo. Si G tiene p-longitud l, entonces G tiene al menos 2^l caracteres irreducibles de grado no divisible por p que toman valores en $\mathbb{Q}_p$.*

Como consecuencia de la demostración del teorema anterior, es posible relacionar el número de clases de conjugación de p-elementos en un grupo p-resoluble G que tienen cuerpo de valores incluido en $\mathbb{Q}_p$, con la p-longitud de G, si p es un primo impar.

Los resultados sobre 2-longitud y caracteres racionales que acabamos de exponer han sido publicados en [34]. En [33] puede encontrarse la generalización del Teorema B a primos arbitrarios y grupos p-resolubles.

2-Grupos con pocas clases de conjugación racionales

Los grupos finitos de orden una potencia de dos y clase de nilpotencia maximal aparecen de manera natural en muchas situaciones en Teoría de Grupos. Recordemos que esta familia de grupos es infinita, dado que para toda potencia 2^a mayor que cuatro, existen grupos de clase maximal que tienen orden 2^a. Es bien conocido que los únicos grupos no abelianos de orden 8 son el grupo diédrico y el grupo cuaternio, y si 2^a es una potencia de dos mayor que 8, entonces hay exactamente tres (tipos de isomorfía de) grupos de clase maximal que tienen orden 2^a. Obviamente, estos grupos son los 2-grupos diédrico, semidiédrico y cuaternio generalizado.

Los 2-grupos diédrico, semidiédrico y cuaternio generalizado admiten un buen número de caracterizaciones, algunas de ellas ampliamente conocidas. Una de estas caracterizaciones, que involucra caracteres racionales, sirve de motivación del resultado principal del

Capítulo 4. Es fácil comprobar que los 2-grupos de clase maximal tienen exactamente 5 caracteres racionales irreducibles, y los autores de [20] demostraron que de hecho ésta es una condición necesaria y suficiente.

Dado que los 2-grupos diédrico, semidiédrico y cuaternio generalizado tienen exactamente 5 clases de conjugación racionales, parece natural esperar que esta sea también una condición necesaria y suficiente, como conjeturó G. Navarro.

Teorema C. *Sea G un 2-grupo con exactamente 5 clases de conjugación racionales. Entonces G es diédrico, semidiédrico o cuaternio generalizado.*

El procedimiento para probar el Teorema C consiste en reducir el problema a una cuestión de grupos metacíclicos, y entonces hacer uso de una clasificación de N. Blackburn de los grupos no metacíclicos minimales, entre otros resultados. Más concretamente, en el Capítulo 4 se clasifican los 2-grupos metacíclicos no abelianos en cuatro familias, y se deduce de esta clasificación que el resultado del Teorema C es cierto para grupos metacíclicos. En particular, es suficiente probar que un 2-grupo con 5 clases de conjugación racionales es metacíclico para obtener el Teorema C en toda su generalidad.

En el artículo [20], el primer paso en la demostración del hecho que los 2-grupos con 5 caracteres irreducibles racionales tienen clase maximal consiste en determinar los 2-grupos con exactamente 4 caracteres racionales irreducibles. En el Capítulo 4, también se caracterizan los 2-grupos con cuatro clases de conjugación racionales, pero el Teorema C es independiente de este resultado.

Es sencillo demostrar que un 2-grupo no puede tener tres caracteres racionales irreducibles. Análogamente, tenemos el siguiente resultado para clases racionales.

Teorema. *Sea G un 2-grupo. El número de clases de conjugación racionales de G no es igual a 3.*

En contraste con el resultado correspondiente sobre caracteres racionales, la demostración del teorema anterior no es completamente trivial; este hecho puede servir para ilustrar la diferencia entre las técnicas utilizadas en [20] y las usadas en el Capítulo 4.

Los resultados que acabamos de describir en esta sección sobre 2-grupos con pocas clases de conjugación racionales han sido obtenidos por el autor y J. Sangroniz, y han sido publicados en [32].

Grupos resolubles con caracteres racionales o cuadráticos

Un grupo finito G se llama **racional** si todos sus caracteres son racionales. Existen resultados en la literatura especializada que estudian los grupos racionales, y más generalmente los grupos con cuerpos de valores *pequeños*. Un modo frecuente de atacar este tipo de problemas consiste en analizar los factores que aparecen en las series de composición de los grupos bajo consideración.

En cierto sentido, para un grupo resoluble G, clasificar los factores que aparecen en una serie de composición de G equivale a determinar los primos que dividen el orden

de G. En el artículo [9], R. Gow demostró que el orden de un grupo resoluble racional sollo puede ser divisible por los primos 2, 3 y 5. Un resultado relacionado es la cota más general que E. Farias e Soares proporcionó en [6], independiente de los resultados de R. Gow, para el conjunto de primos que dividen el orden de un grupo resoluble, en función del menor cuerpo en el que toman valores todos los caracteres de G.

Es interesante hacer notar que la cota obtenida por E. Farias e Soares no se puede mejorar significativamente, en el sentido que es polinómica de grado dos, y no existe ninguna cota lineal de la misma naturaleza (ver [6]). A pesar de ello, aparentemente el resultado de R. Gow no se deduce a partir de la cota de [6].

En el trabajo más reciente [3], D. Chillag y S. Dolfi estudian los grupos resolubles que satisfacen la condición de que cada una de sus clases de conjugación es racional o cuadrática. Como demuestran estos autores, un grupo que cumple esta condición tiene orden solo divisible por primos del conjunto $\{2, 3, 5, 7, 13, 17\}$. En el Capítulo 5 se trata el problema dual para caracteres irreducibles. Recordemos que un carácter $\chi \in \mathrm{Irr}(G)$ es **cuadrático** si

$$|\mathbb{Q}(\chi) : \mathbb{Q}| = 2\,.$$

El teorema principal que se demuestra en el Capítulo 5 es el siguiente.

Teorema D. *Sea G un grupo resoluble tal que sus caracteres irreducibles son racionales o cuadráticos, y sea p un divisor primo de $|G|$. Entonces $p \in \{2, 3, 5, 7, 13\}$.*

Observamos que si p pertenece a $\{2, 3, 5, 7, 13\}$, entonces el grupo de Frobenius G de orden $|G| = p(p-1)/2$ satisface la condición de que todo $\chi \in \mathrm{Irr}(G)$ es racional o cuadrático, luego el Teorema D no puede mejorarse eliminando alguno de los primos de la lista del enunciado.

Algunos de los argumentos usados en el Capítulo 5 dependen del análisis de acciones (de grupos) sin puntos fijos en espacios vectoriales definidos sobre cuerpos de característica positiva, y aquí el uso de la teoría de los caracteres modulares de Brauer parece necessario.

El Teorema D se puede generalizar, obteniendo una cota para el conjunto de primos que dividen el orden de un grupo resoluble G, los caracteres del cual tienen cuerpos de valores que son extensiones de grado acotado sobre $\mathbb{Q}$. Este resultado proporciona una respuesta afirmativa a una cuestión planteada por A. Moretó.

Teorema E. *Existe una función $f : \mathbb{N} \to \mathbb{N}$ tal que para todo grupo G resoluble y todo divisor primo p de $|G|$, si $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ para todo $\chi \in \mathrm{Irr}(G)$ entonces $p \leq f(k)$.*

El **cuerpo de valores** de un grupo finito G se define como el menor cuerpo $\mathbb{Q}(G)$ que contiene los valores de todos los caracteres de G. Una consecuencia del Teorema E es que si G es resoluble con $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ para todo $\chi \in \mathrm{Irr}(G)$, entonces el grado $|\mathbb{Q}(G) : \mathbb{Q}|$ también está acotado por una función que depende solamente de k. Observamos que el Teorema E puede verse como una mejora del resultado principal de [6], que establece que si G es resoluble entonces los primos que dividen $|G|$ están acotados por una función que depende de $|\mathbb{Q}(G) : \mathbb{Q}|$.

Por último, en el Capítulo 5 se da una respuesta afirmativa a una cuestión propuesta en [3] sobre el cuerpo de valores de un grupo resoluble G que satisface que cada una de sus clases de conjugación es racional o cuadrática.

Los resultados principales expuestos en esta sección han sido obtenidos por el autor y pueden encontrarse en [35].

Resum

Introducció

Una qüestió fonamental en la Teoria de Caràcters de Grups Finits consisteix en estudiar la informació sobre l'estructura d'un grup finit que està continguda en la seva taula de caràcters irreductibles. Les entrades que apareixen en la taula de caràcters poden estudiar-se des de distints punts de vista, els quals estan sovint estretament relacionats entre sí.

Tal i com il·lustren els resultats en la literatura especialitzada, el conjunt dels graus dels caràcters irreductibles d'un grup finit (primera columna de la taula de caràcters del grup), conté informació no trivial sobre l'estructura del grup. El teorema d'Ito-Michler (si un primer p no divideix els graus dels caràcter irreductibles de G, llavors G té un p-subgrup de Sylow normal), és un exemple molt destacable d'aquest tipus de resultats, en els quals consideracions de tipus artimètic són sovint rellevants. Un altre focus d'interés en investigacions recents en Teoria de Caràcters ha estat el conjunt de zeros en la taula de caràcters d'un grup, així com altres conjunts relacionats, i s'ha comprovat que aquest conjunt també hi reflexa aspectes de l'estructura del grup corresponent.

El punt de vista que nosaltres adoptem en aquesta memòria, el qual ha estat també explorat a la literatura prèviament, és l'anàlisi de cossos de valors de caràcters ordinaris i la seva relació amb certs invariants del grup. En aquest context, les qüestions sobre racionalitat en grups finits es troben probablement entre les més interessants, i veurem que alguns dels nostres resultats tracten problemes que involucren caràcters que prenen valors en el cos dels racionals (**caràcters racionals**) i classes de conjugació que contenen elements racionals (**classes racionals**) en grups finits.

És ben sabut que els caràcters d'un grup finit prenen valors en extensions ciclotòmiques del cos dels nombres racionals, de manera que no resulta sorprenent que la Teoria de Galois jugue un paper important en l'estudi de cossos de valors de grups finits, i en el nostre treball en particular. A mode d'introducció, i donada la seva rellevància en l'obtenció dels nostres resultats, a continuació descriurem com algunes de les tècniques de la Teoria de Galois poden ser aplicades en l'anàlisi de cossos de valors de grups finits. Aquests resultats preliminars poden trobar-se al Capítol 1, on a més s'hi presenten els fonaments i alguns resultats bàsics de la Teoria de Caràcters de Grups Finits que són necessaris al llarg del treball.

Siga G un grup finit. El conjunt de caràcters irreductibles complexos de G és denotat per $\mathrm{Irr}(G)$, i el conjunt de les classes de conjugació de G és designat per $\mathrm{Cl}(G)$. Com és habitual, si g és un element de G, escrivim $\mathrm{Cl}_G(g)$ per a la classe de conjugació de g en G. No és difícil veure que tot caracàcter irreductible de G es pot veure com el caràcter d'una

representació irreductible $\mathcal{X}$ de G sobre un cos E que és una extensió finita de Galois del cos dels racionals $\mathbb{Q}$. A més, es pot suposar que E conté una arrel primitiva n-èssima complexa de la unitat, on n és un múltiple de l'exponent de G. Aquesta observació implica que el grup de Galois $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ actua sobre el conjunt dels caràcters irreductibles de G de manera natural. Més concretament, siguen $\chi \in \mathrm{Irr}(G)$ i $\sigma \in \mathcal{G}_n$. Aleshores definim

$$\chi^\sigma(g) = \chi(g)^\sigma$$

per a tot $g \in G$. Es pot comprovar que efectivament $\chi^\sigma \in \mathrm{Irr}(G)$, i en particular es segueix que $\mathcal{G}_n$ també actua sobre els caràcters no necessàriament irreductibles de G.

Seguint amb la mateixa notació, el grup de Galois $\mathcal{G}_n$ també actua de manera natural sobre el conjunt de les classes de conjugació $\mathrm{Cl}(G)$ de G. Per teoria elemental de cossos, un automorfisme $\sigma \in \mathcal{G}_n$ està unívocament determinat per un enter t, que és coprimer amb n i únic mòdul n, tal que t satisfà l'equació $\xi^\sigma = \xi^t$ per a qualsevol arrel n-èssima primitiva de la unitat $\xi \in \mathbb{C}$. Siga g un element de G. Llavors escrivim

$$\mathrm{Cl}_G(g)^\sigma = \mathrm{Cl}_G(g^t)\,,$$

i es pot veure fàcilment que aquesta expressió defineix una acció de $\mathcal{G}_n$ sobre les classes de conjugació de G.

Les accions de $\mathcal{G}_n$ sobre $\mathrm{Irr}(G)$ i sobre $\mathrm{Cl}(G)$ no són isomòrfiques com a permutacions en general, tot i que estan estretament relacionades. Pel Lema de les Permutacions de Brauer, un automorfisme qualsevol $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ fixa el mateix nombre de caràcters irreductibles de G que de classes de conjugació de G. En particular, en un grup finit qualsevol G, el nombre de caràcters que prenen només valors reals (**caràcters reals**) coincideix amb el nombre de classes de conjugació en les què tots els caràcters de G prenen valors reals (**classes reals**), ja que els caràcters i les classes reals són exactaments aquells fixats per la conjugació complexa.

Siga $\chi \in \mathrm{Irr}(G)$. El **cos de valors** de χ en G és, per definició, el mínim cos que conté tots els valors que pren el caràcter χ en el grup G, és a dir

$$\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g) \mid g \in G)\,.$$

De manera similar, si $g \in G$, **el cos de valors** de g en G es defineix com

$$\mathbb{Q}(g) = \mathbb{Q}(\chi(g) \,|\, \chi \in \mathrm{Irr}(G))\,,$$

és a dir, és el menor cos que conté els valors que els caràcters de G prenen en g. Sovint escrivim $\mathbb{Q}(g) = \mathbb{Q}(C)$, on C és la classe de conjugació de g en G.

Remarquem que és una conseqüència immediata de les definicions de cossos de valors de caràcters i classes, que l'estabilitzador d'un caràcter $\chi \in \mathrm{Irr}(G)$ en l'acció natural de $\mathcal{G}_n$ és precisament

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(\chi))\,,$$

mentre que l'estabilitzador d'una classe de conjugació $C \in \mathrm{Cl}(G)$ és

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(C)).$$

En particular un caràcter $\chi \in \mathrm{Irr}(G)$ és racional si i només si χ és $\mathcal{G}_n$-invariant, i el mateix ocorre per a les classes de conjugació $C \in \mathrm{Cl}(G)$.

Racionalitat i 2-subgrups de Sylow

Suposem que n és un múltiple de l'exponent d'un grup G. Les accions del grup de Galois $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ sobre els caràcters irreductibles de G i sobre el conjunt de les classes de conjugació G no són isomorfes en general, tal i com hem indicat abans. Els grups de menor ordre on les dues accions no són isomorfes tenen 2^5 elements. Observem que pels aguments exposats a la secció anterior, quan aqeustes dues accions són isomorfes, existeix una bijecció entre les classes de conjugació i els caràcters irreductibles de G que preserva els cossos de valors. En particular, en aquest cas tenim que el nombre de classes de conjugació racionals de G és igual al nombre de caràcters irreductibles racionals de G.

És important adonar-se'n que pot ocorrer que G tinga el mateix nombre de classes i caràcters racionals, però que les accions de $\mathcal{G}_n$ sobre $\mathrm{Irr}(G)$ i sobre $\mathrm{Cl}(G)$ no siguen isomorfes, com ho demostren certs grups d'ordre senar, per exemple.

Una conseqüència del resultat principal de [2], és que un grup G té el mateix nombre de classes racionals que de caràcters irreductibles racionals si tots els subgrups se Sylow de G són abelians, ja que sota aquestes condicions les accions de $\mathcal{G}_n$ sobre $\mathrm{Irr}(G)$ i sobre $\mathrm{Cl}(G)$ són isomorfes. Una altra condició suficient per obtindre la igualtat entre el nombre de classes de conjugació racionals i el nombre de caràcters irreductibles racionals d'un grup finit s'hi pot trobar a [31]: la igualtat és certa si qualsevol d'aquests nombres és igual a 2.

Al Capítol 2 d'aquesta memòria, comptem les classes racionals i els caràcters racionals de grups que tenen un 2-subgrup de Sylow cíclic, i obtenim el següent resultat, que és el teorema principal del capítol.

Teorema A. *Suposem que G té un 2-subgrup de Sylow P cíclic. Aleshores G té el mateix nombre de classes racionals que de caràcters irreductibles racionals.*

Malauradament, el Teorema A sembla no obrir un ventall de resultats del mateix tipus. De fet, si canviem a l'enunciat la condició que P siga cíclic per $P = C_2 \times C_2$, on C_2 és el grup cíclic d'order 2, llavors el Teorema A és fals, fins i tot si assumim que G té un 2-complement normal, com ho prova el fet que existeix un grup d'ordre $2^2 \cdot 3^4 \cdot 7$ que té un 2-subgrup de Sylow elemental abelià, un 2-complement normal i un nombre de classes racionals distint del nombre de caràcters racionals.

La demostració del Teorema A no és en absolut elemental, a pesar que les hipòtesis poden semblar fortes. Per tal d'obtindre el resultat, és necessari emprar la π-teoria d'Isaacs, la correspondència de Glauberman-Isaacs i alguns dels arguments de l'article sobre caràcters quadràtics en grups d'ordre senar [28], entre d'altres. Els mètodes emprats al Capítol 2 són presentats amb la suficient generalitat perquè puguen aplicar-se en altres punts del treball (especialment al Capítol 5), i permeten també analitzar sota

quines condicions grups amb un p-subgrup de Sylow normal tenen el mateix nombre de classes i caràcters racionals. El següent resultat també apareix al Capítol 2 de la tesi.

Teorema. *Suposem que $G = PQ$, on $P \lhd G$ és un p-subgrup de Sylow de G, per a p un primer senar, i Q és un 2-grup abelià, dièdric, semidièdric o quaternió generalitzat. Llavors G té el mateix nombre de classes racionals que de caràcters irreductibles racionals.*

La demostració del teorema anterior depén, a més dels resultats previs emprats per obtindre el Teorema A, de l'existència d'una correspondència natural entre les classes de conjugació racionals i els caràcters irreductibles racionals d'un 2-grup dièdric, semidièdric o quaternió generalitzat.

Els resultats nous presentats en aquesta secció són treball conjunt de l'autor i G. Navarro, i han estat publicats a [30].

2-Longitud i caràcters racionals de grau senar

És un fet ben conegut que un grup finit G té ordre senar si i només si G té un únic caràcter irreductible racional. Un refinament d'aquest resultat va ser conjecturat per R. Gow, qui va predir que tot grup finit d'ordre parell té un caràcter irreductible racional no trivial de grau senar.

Recentment, G. Navarro i P. H. Tiep van demostrar que la conjectura de R. Gow és certa a [31]. Per tal de provar la conjectura, els autors van introduir noves tècniques d'extensió de caràcters racionals, que van permetre demostrar una versió més forta del resultat per a grups resolubles. Més concretament, G. Navarro i P. H. Tiep mostraren que si G és un grup resoluble d'ordre parell, llavors la 2-longitud de G és menor que el nombre de caràcters irreductibles racionals de G de grau senar.

El nostre principal objectiu al Capítol 3 és obtindre una millora significativa del resultat de G. Navarro i P. H. Tiep que acabem d'esmentar. Podem demostrar que existeix una cota superior logarítmica per a la 2-longitud d'un grup resoluble G, en termes del nombre de caràcters irreductibles racionals de grau senar de G.

Teorema B. *Siga G un grup resoluble d'ordre parell, i suposem que la 2-longitud de G és $l \in \mathbb{N}$. Aleshores G té com a mínim 2^l caràcters racionals de grau senar.*

Entre les implicacions d'aquest resultat, hi trobem una nova relació local/global, tal vegada no esperada, que no involucra caràcters a l'enunciat. Com és habitual, denotem per $\Phi(P)$ el subgrup de Frattini d'un grup P.

Corol·lari. *Siga P un 2-subgrup de Sylow de G. Llavors el nombre d'òrbites de l'acció del normalitzador $\mathbf{N}_G(P)$ per conjugació sobre $P/\Phi(P)$ admet una cota inferior logarítmica en termes de la 2-longitud de G.*

Vegem ara altres aplicacions del Teorema B. És una conseqüència immediata d'un teorema de J. Thompson (veure IX.8.6 de [12]) que un grup resoluble amb únicament dues classes de conjugació racionals té 2-longitud 1. Recentment, M. Isaacs i G. Navarro

provaren en [18] que la mateixa conclusió és certa per a un grup resoluble G que té com a màxim tres classes de conjugació d'elements racionals. Tal i com els autors de [18] mostren, aquest resultat pot deduir-se a partir del Teorema B.

Sembla natural preguntar-se si la cota que el Teorema B proporciona és de fet una cota òptima. Al Capítol 3 construim una successió de grups resolubles

$$G_1, G_2, \ldots, G_l, \ldots$$

tal que G_l té 2-longitud l i exactament 2^l caràcters irreductibles racionals de grau senar, de manera que la cota del Teorema B no es pot millorar.

Finalment, el Teorema B admet la següent generalització per a nombres primers arbitraris p i grups p-resolubles. En la demostració d'aquesta versió més general hem utilitzat novament la teoria dels caràcters B_p d'Isaacs. Igual que abans, si n és un enter qualsevol, llavors $\mathbb{Q}_n$ és la n-èssima extensió ciclotòmica sobre $\mathbb{Q}$.

Teorema. *Siga G un grup p-resoluble, on p és un primer. Si G té p-longitud l, llavors G té almenys 2^l caràcters irreductibles de grau no divisible per p que prenen valors en $\mathbb{Q}_p$.*

Com a conseqüència de la demostració del teorema anterior, és possible relacionar el nombre de classes de conjugació de p-elements d'un grup p-resoluble G que tenen cos de valors inclòs en $\mathbb{Q}_p$, amb la p-longitud de G, si p és un primer senar.

Els resultats sobre 2-longitud i caràcters racionals que acabem d'exposar han estat publicats a [34]. Veure també [33].

2-Grups amb poques classes de conjugació racionals

Els grups finits d'ordre una potència de dos i classe de nilpotència maximal apareixen de manera natural en moltes situacions en Teoria de Grups. Tal vegada, el primer fet que calga recordar sobre aquesta família de grups és que és infinita, donat que per a tota potència 2^a major que quatre, existeixen grups de classe maximal que tenen ordre 2^a. És ben sabut que els únics grups no abelians d'ordre 8 són el grup dièdric i el quaternió, i si 2^a és una potència de dos major que 8, aleshores hi ha exactament tres (tipus d'isomorfia de) grups de classe maximal que tinguen ordre 2^a. Òbviament, aquests grups són el 2-grups dièdric, semidièdric i quaternió generalitzat.

Els 2-grups dièdric, semidièdric i quaternió generalitzat admeten un bon nombre de caracteritzacions, algunes d'elles amplament conegudes. Una d'aquestes caracteritzacions, què involucra caràcters racionals, serveix de motivació del resultat principal del Capítol 4. És fàcil comprovar que els 2-grups de classe maximal tenen exactament 5 caràcters irreductibles racionals, i els autors de [20] demostraren que de fet aquesta és una condició necessària i suficient.

Donat que els 2-grups dièdric, semidièdric i quaternió generalitzat tenen exactament 5 classes de conjugació racionals, sembla natural esperar que aquesta siga també una condició necessària i suficient, tal i com va ser conjecturat per G. Navarro.

Teorema C. *Siga G un 2-grup amb exactament 5 classes de conjugació racionals. Llavors G és dièdric, semidièdric o quaternió generalitzat.*

El procediment per a provar el Teorema C consisteix en reduir el problema a una qüestió de grups metacíclics, i llavors emprar una classificació de N. Blackburn dels grups no metacíclics minimals, entre altres resultats. Més concretament, al Capítol 4 s'hi classifiquen els 2-grups metacíclics no abelians en quatre famílies, i es dedueix d'aquesta classificació que el resultat del Teorema C és cert per a grups metacíclics. En particular, és suficient provar que un 2-grup amb 5 classes de conjugació racionals és metacíclic per tal d'obtindre el Teorema C en tota la seva generalitat.

En l'article [20], el primer pas en la demostració que els 2-grups amb 5 caràcters irreductibles racionals tenen classe maximal consisteix en determinar els 2-grups amb exactament 4 caràcters racionals irreductibles. Al Capítol 4, també es caracteritzen els 2-grups amb quatre classes de conjugació racionals, però el Teorema C és independent d'aquest resultat per a classes racionals.

És senzill demostrar que un 2-grup no pot tindre tres caràcters racionals irreductibles. Anàlogament, tenim el següent resultat.

Teorema. *Siga G un 2-grup. Aleshores el nombre de classes de conjugació racionals de G no és igual a 3.*

Contràriament al cas que tracta caràcters racionals, el teorema anterior no és completament trivial, i la seva demostració és un bon exemple de la diferència en les tècniques utilitzades en [20] i aquelles introduides al Capítol 4.

Els resultats que esmentats sobre 2-grups amb poques classes de conjugació racionals en aquesta secció són treball conjunt de l'autor i J. Sangroniz, i han estat publicats a [32].

Grups resolubles amb caràcters racionals o quadràtics

Un grup finit G es diu que és **racional** si tots els seus caràcters són racionals. Diversos resultats a la literatura especialitzada estudien grups racionals, i més en general grups amb cossos de valors *menuts*. Una via freqüent d'atacar aquest tipus de problemes consisteix en analitzar els factors que apareixen a una sèrie de composició d'un grup pertanyent a la família que és objecte d'estudi.

En certa mesura, per a un grup resoluble G, classificar els factors que apareixen en una sèries de composició equival a determinar els primers que divideixen l'ordre de G. A l'article [9], R. Gow demostrà que l'ordre d'un grup resoluble racional només pot ser divisible pels primers 2, 3 i 5. Un resultat relacionat és la cota més general que E. Farias e Soares proporcionà en [6], independent dels resultats de R. Gow, per al conjunt de primers que divideixen l'ordre d'un grup resoluble, en termes del menor cos on prenen valors tots els caràcters de G.

És interessant notar que la cota donada per E. Farias e Soares no es pot millorar significativament, en el sentit que és polinòmica de grau dos, i no existeixen cotes lineals

de la mateixa natura. Tot i això, el resultat de R. Gow no es dedueix a partir de la cota de [6].

Al treball més recent [3], realitzat per D. Chillag i S. Dolfi, s'hi estudien els grups resolubles que satisfan la condició que cadascuna de les seves classes de conjugació és o bé racional o bé quadràtica. Tal i com demostren aquests autors, un grup pertanyent a aquesta família té ordre només divisible per primers al conjunt $\{2, 3, 5, 7, 13, 17\}$. Al Capítol 5 s'hi tracta el problema dual per a caràcters irreductibles. Recordem que un caràcter $\chi \in \mathrm{Irr}(G)$ és **quadràtic** si

$$|\mathbb{Q}(\chi) : \mathbb{Q}| = 2 .$$

El teorema principal que s'hi demostra al Capítol 5 és el següent.

Teorema D. *Siga G un grup resoluble tal que els seus caràcters irreductibles són o bé racionals o bé quadràtics, i siga p un divisor primer de $|G|$. Llavors $p \in \{2, 3, 5, 7, 13\}$.*

Observem que si p pertany a $\{2, 3, 5, 7, 13\}$, llavors el grup de Frobenius G d'ordre $|G| = p(p-1)/2$ satisfà que tot $\chi \in \mathrm{Irr}(G)$ és racional o quadràtic, i llavors el Teorema D no pot millorar-se eliminant algun primer de la llista de l'enunciat.

Alguns dels arguments que apareixen al Capítol 5 depenen de l'anàlisi d'accions sense punts fixos en espais vectorials definits sobre cossos de característica positiva, i aleshores l'ús de la teoria dels caràcters modulars de Brauer sembla necessari.

El Teorema D es pot generalitzar per tal d'obtindre una cota per al conjunt de primers que divideixen l'ordre d'un grup resoluble G, els caràcters del qual tenen cossos de valors de grau sobre $\mathbb{Q}$ acotat, resultat que proporciona una resposta positiva a una qüestió plantejada per A. Moretó.

Teorema E. *Existeix una funció $f : \mathbb{N} \to \mathbb{N}$ tal que si G és un grup resoluble que satisfà $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$, per a tot $\chi \in \mathrm{Irr}(G)$, i p és un divisor primer de $|G|$, llavors $p \leq f(k)$.*

El **cos de valors** d'un grup finit G és el mínim cos $\mathbb{Q}(G)$ que conté els valors de tots els caràcters de G. Una conseqüència del Teorema E és que si G és resoluble amb $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ per a tot $\chi \in \mathrm{Irr}(G)$, llavors el grau $|\mathbb{Q}(G) : \mathbb{Q}|$ també està acotat per una funció que depén només de k. Observem que el Teorema E es pot veure com una millora del resultat principal de [6], que estableix que si G és resoluble llavors els primers que divideixen $|G|$ estan acotats per una funció que depén de $|\mathbb{Q}(G) : \mathbb{Q}|$.

Per acabar, al Capítol 5 es dóna una resposta afirmativa a una qüestió proposada a [3] sobre el cos de valors d'un grup resoluble G que satisfà que cadascuna de les seves classes de conjugació és o bé racional o bé quadràtica.

Els resultats principals exposats en aquesta secció han sigut obtinguts per l'autor i poden trobar-se a [35].

Introduction

A fundamental question in the Character Theory of Finite Groups is to reveal what information about a group is encoded in its character table. Indeed, the data appearing in the character table of a group has been studied from several perspectives, which are closely interrelated.

For instance, a variety of results shows that the irreducible character degrees (first column in the character table) of a finite group contain a great amount of non-trivial information about the group. Like in the celebrated Ito-Michler theorem (if a prime p does not divide the irreducible character degrees of G, then G has a normal Sylow p-subgroup), arithmetical considerations often arise in this approach. Another focus of interest in recent research, for instance, has been the set of zeros appearing in the character table of a group, which also reflects and is reflected in the structure of the group.

Certainly, the point of view that we adopt in this work has been explored in the literature too. We analyze fields containing values of ordinary characters and their relationship with a number of invariants of the group. Within this frame, rationality questions are probably among the most interesting, and we devote several results to problems involving rational characters and conjugacy classes containing rational elements (rational classes) of finite groups.

As ordinary characters take values in cyclotomic fields, it is not surprising that Galois theory becomes relevant in our work. The Galois group $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, where n is the order of a finite group G, permutes naturally the set of irreducible characters of G, as well as the set of its conjugacy classes, and when these two actions are isomorphic then we know that there is a bijection between field of values of characters and field of values of classes. In particular, the number of rational characters is the number of rational classes in this case. An old theorem of A. Broshi [2] asserts that both actions are isomorphic if all the Sylow subgroups of G are abelian.

Unfortunately, there are no more general results of this type in the literature. Results guaranteeing that the number of rational classes and rational characters coincide are also very rare (another one is provided in recent work by G. Navarro and P. H. Tiep [31]). Since this is definitely the case in groups of odd order, because groups of odd order do not possess rational classes or rational characters except the trivial ones, we study in Chapter 2 finite groups in which a Sylow 2-subgroup P of G is under tight control. We are able to prove, among some other results, that if P is cyclic, then G has the same number of irreducible rational characters and rational conjugacy classes. This constitutes Theorem A and has been published in a joint paper by the author and G. Navarro [30].

We remark that the proof of Theorem A is not elementary at all, despite the strength of

the hypothesis. Actually, it requires the use of Isaacs deep π-theory, character correspondences and arguments from the paper on quadratic characters of odd-order groups [28]. As it is natural to expect, some of the techniques used to prove Theorem A depend on the fact that a group with a cyclic Sylow 2-subgroup possesses a normal 2-complement, and consequently some results about fields of values and normal subgroups are developed; this more general machinery on normal subgroups can also be used to attack other problems, like those in Chapter 5.

It is a well-known fact that finite groups of even order always possess non-trivial irreducible rational characters; this was recently refined by G. Navarro and P. H. Tiep [31], who proved that a group of even order always has a non-trivial irreducible rational character of odd degree, giving therefore a positive answer to an old conjecture by R. Gow.

In fact, it seems that rational characters of odd degree somehow reflect features of the structure of a group that are related to the prime number 2. We explote this fact in Chapter 3, showing that the 2-length of a solvable group G admits an upper logarithmic bound by the number of irreducible rational characters of odd degree of G. This improves a result by G. Navarro and P. H. Tiep in [31]. It is probably worth it mentioning that this new bound, which constitutes Theorem B and has been published in [34], has been used by G. Navarro and M. Isaacs in their recent work [18] on solvable groups having three rational conjugacy classes of 2-elements.

The main result in Chapter 3 is a version for conjugacy classes of a theorem of M. Isaacs, G. Navarro and J. Sangroniz [20] on 2-groups with 5 rational irreducible characters. More precisely, Theorem C characterizes dihedral, semi-dihedral and generalized quaternion 2-groups as those 2-groups having precisely 5 conjugacy classes of rational elements. In addition, 2-groups with 4 rational classes are characterized, and it is shown that a group of order a power of 2 cannot have exactly 3 rational classes. The strategy to prove Theorem C consists in reducing the problem to metacyclic 2-groups, and then make use of a classification of minimal non-metacyclic 2-groups carried out by N. Blackburn (see Theorem 66.1 of [1]), among other facts. All these results on 2-groups with few rational classes are joint work of the author and J. Sangroniz, and have been published in [32].

In general, the techniques applied in Chapter 3 differ from those in [20], the main reason being perhaps that rational classes do not have a good behavior when passing to quotient groups, as it is the case for characters. Instead, the analysis of groups generated by few conjugacy classes of rational 2-elements becomes essential in the proof of Theorem C.

Recall that a group is called rational if all its characters are rational-valued. Rationality in a finite group G is belived to be somehow related to the Sylow 2-subgroups of G, and in fact it remained as a long open question to determine whether the Sylow 2-subgroups of a rational group were themselves rational (a counterexample was recently found by G. Navarro and M. Isaacs in [19]).

A series of results in the literature deals with finite rational groups, and more generally with groups with small fields of values. A common approach to the study of these groups consists on analyzing the composition factors of groups in the family under consideration, which is frequently assumed to contain only solvable groups. Indeed, we proceed in such

a way in Chapter 5, proving that solvable groups all whose characters are either rational or quadratic have order only divisible by primes smaller than 19; this is Theorem D.

Some of the arguments used in Chapter 5 involve the analysis of certain fixed-point-free actions on vector spaces over fields of positive characteristic, and an appeal to Brauer theory of modular characters seems necessary at that point.

It might be convenient to put Theorem D above into context. R. Gow showed in his important paper [9] that rational solvable groups are only divisible by the primes 2, 3 or 5, while E. Farias e Soares gave in [6] a more general bound of the same nature, which we improve in Theorem E in a certain sense (Chapter 5). In a similar fashion, D. Chillag and S. Dolfi treated the dual of Theorem D for conjugacy classes of solvable groups [3], being our results similar and independent from those in [3]. In the more general setting of not necessarily solvable groups, the work [7] by W. Feit and G. Seitz classifies the non-abelian chief factors of rational groups, while J. Thompson studied the cyclic composition factors of a rational group in [36], being still an open problem to show that 7 and 11 cannot appear as the order of a cyclic composition factor of such a group. Both Theorem D and Theorem E appear in [35].

We mention that Chapter 1 is devoted to remind the reader of some known preliminary results which are needed for the proof of the main results in the dissertation.

Part of this work was done at the University of Wisconsin, Madison, where I did research under the supervision of M. Isaacs for an academic year; at the Universidad del País Vasco, which I visited to work with J. Sangroniz for two weeks; at the Universita di Firenze, where I was under the guidance of S. Dolfi for two weeks; and at the University of Aberdeen, where I spent three months under the supervision of G. Robinson. I want to express here my gratitude to all of them for their hospitality, help and guidance in my research.

I also want to thank A. Moretó for many helpful conversations and his support, and of course G. Navarro, my advisor, who always supported me and made this dissertation possible.

Chapter 1

Preliminary results

Unless otherwise is stated, all groups considered are finite.

1.1 Representations, modules and characters

Suppose that G is a group and F is an arbitrary field. The **group algebra** $F[G]$ consists of the formal sums

$$\sum_{g \in G} a_g g \,,$$

where $a_g \in F$ for all $g \in G$. The elements of G can be viewed as elements of the algebra $F[G]$, and in fact they form an F-basis for $F[G]$. Multiplication in $F[G]$ of the elements of this basis is defined like the product of elements in G; then, this multiplication is extended by linearity to the whole algebra $F[G]$.

An F-**representation** of G is an algebra homomorphism $\mathcal{X} : F[G] \to M_n(F)$, where $M_n(F)$ is the algebra of square matrices of size $n \times n$ with entries in the field F. The positive integer n is the **degree** of the representation $\mathcal{X}$. It is clear that the restriction

$$\hat{\mathcal{X}} : G \longrightarrow \mathrm{GL}(n, F)$$

is a well-defined group homomorphism, where $\mathrm{GL}(n, F)$ is the group of invertible matrices of size $n \times n$ with entries in F, and $\hat{\mathcal{X}}$ completely determines the representation $\mathcal{X}$ by linearity. Then, we often identify $\mathcal{X}$ with its restriction to G.

Two F-representations $\mathcal{X}$ and $\mathcal{Y}$ of G are **similar** if there exists $M \in \mathrm{GL}(n, F)$ such that $\mathcal{Y}(g) = M^{-1}\mathcal{X}(g)M$, for all $g \in G$. It is clear that similarity defines an equivalence relation on the F-representations of G.

Let us recall the definition of an $F[G]$-module. Let V be a finite dimensional F-vector space, and suppose that for every $v \in V$ and $x \in F[G]$ it is defined a unique vector $vx \in V$. Assume for all $x, y \in F[G]$, $v, w \in V$, and $c \in F$ that

1. $(v + w)x = vx + wx$,
2. $v(x + y) = vx + vy$,

3. $(vx)y = v(xy)$,
4. $(cv)x = c(vx) = v(cx)$,
5. $v1 = v$.

Then V is called an $F[G]$-**module**. When there is no possible confussion, we may just say that V is a module of the group G.

Recall that a subspace U of an $F[G]$-module V is an $F[G]$-**submodule** of V provided that $ux \in U$, for all $u \in U$ and all $x \in F[G]$. In this case, the quotient space V/U is also an $F[G]$-module in a natural way. The module V is **simple** or **irreducible** if V is nonzero and its unique submodules are 0 and V.

Observe that an F-representation $\mathcal{X}$ of G naturally gives rise to an $F[G]$-module. Indeed, if $\mathcal{X}$ has degree n, consider the canonical F-vector space $V = F^n$. Then we can define an action of G on V by setting

$$v \cdot a = v\mathcal{X}(a)\,,$$

for $v \in V$ and $a \in G$, and it is routine to check that this endows V with the structure of an $F[G]$-module, extending the action to the whole algebra $F[G]$ by linearity.

Conversely, suppose that V is an $F[G]$-module. Then every element $g \in G$ defines an F-endomorphism f_g of V via $v \mapsto v \cdot g$, and we let M_g be the matrix associated to f_g with respect to a fixed F-basis for V. Since $(f_g)^{-1} = f_{g^{-1}}$, all matrices M_g obtained in this way are invertible. Now, it is not difficult to check that the map

$$\begin{array}{ccc} G & \longrightarrow & \mathrm{GL}(n, F) \\ g & \mapsto & M_g \end{array}$$

is a group homomorphism, i .e. an F-representation of G. Of course, isomorphic $F[G]$-modules afford similar representations, and viceversa.

We recall that an F-representation of G is **irreducible** if it is afforded by an irreducible $F[G]$-module.

Suppose now that $V \neq 0$ is an $F[G]$-module and let

$$0 = V_0 < V_1 < \cdots < V_i < \cdots < V_n = V$$

be a chain of submodules of V. If each quotient module V_i/V_{i-1} is simple for $1 \leq i \leq n$, then the chain of submodules is called a **composition series** of V. The Jordan-Hölder theorem asserts that the factors V_i/V_{i-1} appearing in two distinct composition series of V are the same up to isomorphism (and counting multiplicities).

Observe that it is clear that if $\mathcal{X}$ is a representation of G afforded by V, then $\mathcal{X}$ is similar to an upper triangular representation $\mathcal{Y}$ in block form

$$\mathcal{Y}(g) = \begin{pmatrix} \mathcal{Y}_1(g) & & & * \\ & \mathcal{Y}_2(g) & & \\ & & \ddots & \\ 0 & & & \mathcal{Y}_n(g) \end{pmatrix}$$

for every $g \in G$, where $\mathcal{Y}_i$ is an F-representation of G afforded by V_i/V_{i-1}. These representations $\mathcal{Y}_i$ of G are called the **irreducible constituents** of $\mathcal{X}$, and by the Jordan-Hölder theorem they are uniquely determined up to similarity.

If $\mathcal{X}$ is an F-representation of G, then the **F-character** χ of G afforded by $\mathcal{X}$ is the map sending each element $x \in F[G]$ to the trace of the matrix $\mathcal{X}(x)$. Since χ is completely determined by its restrictions to G by linearity, we usually consider the character as a map

$$\chi : G \longrightarrow F .$$

An **irreducible character** of G is a character afforded by an irreducible representation of G.

From now on we fix $F = \mathbb{C}$ and unless otherwise is stated when we write "character" we mean "complex character".

The set of irreducible complex characters of a group G is usually denoted by $\mathrm{Irr}(G)$, and by next result it has size equal to the number of conjugacy classes of G.

Theorem 1.1. *The number of irreducible characters of a group G equals the number of conjugacy classes of G.*

Proof. See Corollary 2.7 of [13]. ∎

Recall that a complex **class function** of G is a map

$$\varphi : G \longrightarrow \mathbb{C}$$

which is constant on the conjugacy classes of G, and the set of complex class functions of G is denoted by $\mathrm{cf}(G)$. It is easily seen that characters of G lie in $\mathrm{cf}(G)$, which of course has the structure of a vector space over $\mathbb{C}$.

Theorem 1.2. *The set* $\mathrm{Irr}(G)$ *is a* $\mathbb{C}$*-basis for* $\mathrm{cf}(G)$.

Proof. See Theorem 2.8 of [13]. ∎

We can arrange the values of the irreducible characters of G in a table whose entries are given by the matrix

$$X(G) = \left(\chi_i(x_j)\right),$$

where $\chi_i \in \mathrm{Irr}(G)$ and the x_j are representatives of the conjugacy classes of G. The table obtained in this way, with rows corresponding to characters and columns to conjugacy classes, is called the **character table** of G. Observe that $X(G)$ is a square matrix by Theorem 1.1, and we note that this matrix is invertible by Theorem 1.2.

We observe that it follows from Theorem 1.2 that every character of G can be uniquely expressed as a linear combination of irreducible characters of G, and in fact the coefficients appearing in this linear combination are non-negative integers, by Theorem 2.8 of [13]. Assume that χ is a character of G and write

$$\chi = \sum a_\psi \psi ,$$

where $\psi \in \mathrm{Irr}(G)$ and each a_ψ is a non-negative integer. The characters ψ such that $a_\psi \neq 0$ are called the **irreducible consitutents** of χ.

It is convenient to recall that a complex character of G determines the similarity class of the representations of G affording it.

Theorem 1.3. *Let $\mathcal{X}$ and $\mathcal{Y}$ be complex representations of G. Then $\mathcal{X}$ and $\mathcal{Y}$ are similar if and only if they afford the same character.*

Suppose that χ is a character of G. Then the integer $\chi(1)$ is the **degree** of χ, and equals the degree of any representation of G affording χ (this does not hold if the characteristic of F is non-zero). A character of G is called **linear** if it has degree one.

The set of degrees of the irreducible characters of G contains non-trivial information about the structure of G. For instance, the following is a fundamental equality

$$|G| = \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)^2 \tag{1.1}$$

(see Corollary 2.7 of [13]). Observe that it follows from 1.1 and Theorem 1.1 that a group G is abelian if and only if all the irreducible characters of G are linear. We shall use this without further reference.

Another basic relation involving character degrees is the following.

Theorem 1.4. *Let $\chi \in \mathrm{Irr}(G)$. Then $\chi(1)$ divides $|G|$.*

Proof. See Theorem 3.11 of [13]. ∎

Suppose now that $\varphi, \theta \in \mathrm{cf}(G)$ and define the product $\varphi\theta$ via

$$(\varphi\theta)(g) = \varphi(g)\psi(g)\,,$$

where g runs over G. It is immediate to see that the product $\varphi\theta$ also lies in $\mathrm{cf}(G)$. Furthermore, if we take characters of G we have that:

Theorem 1.5. *Products of characters of G are characters of G.*

Proof. See Theorem 4.2 of [13]. ∎

Note that the set of linear characters of a group is a group with the product of characters. If G is an abelian group, then G is isomorphic to $\mathrm{Irr}(G)$.

The inner product of two class functions $\varphi, \theta \in \mathrm{cf}(G)$ is defined by

$$[\varphi, \theta] = \frac{1}{|G|} \sum_{g \in G} \varphi(g)\overline{\theta(g)}\,.$$

It is immediate to check that $[\ ,\ ]$ actually satisfies the axioms of an inner product on the $\mathbb{C}$-vector space $\mathrm{cf}(G)$, and therefore makes the space of class functions of G into a Hermitian space.

By the First Orthogonality Relation (see Corollary 2.14 of [13]) we have that

$$[\chi_i, \chi_j] = \delta_{ij}\,,$$

where $\chi_i, \chi_j \in \mathrm{Irr}(G)$ and δ_{ij} is the Kronecker delta, so $\mathrm{Irr}(G)$ is an orthonormal basis for the space of class functions of G. Thus if $\varphi \in \mathrm{cf}(G)$ with $[\varphi, \chi] = c_\chi$ for $\chi \in \mathrm{Irr}(G)$, then $\varphi = \sum c_\chi \chi$, and the other way around.

For the sake of completeness, we recall that the Second Orthogonality Relation (see Theorem 2.18 of [13]) is a consequence of the first one and it states that for $g, h \in G$

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g)\overline{\chi(h)} = 0$$

if g and h are not conjugate in G; otherwise the sum equals $|\mathbf{C}_G(g)|$.

Let χ be a character of G. The **kernel** of χ is defined as

$$\ker(\chi) = \{g \in G \,|\, \chi(g) = \chi(1)\}\,.$$

Theorem 1.6. *Let χ be a character of G afforded by a representation $\mathcal{X}$ of G. Then $\ker(\chi) = \ker(\mathcal{X})$, so the kernel of χ is a normal subgroup of G.*

Proof. See Theorem 2.19 of [13]. ∎

A character χ of G is called **faithful** if $\ker(\chi)$ is the trivial subgroup of G.

Suppose now that $\mathcal{X}$ is a complex representation of G affording the character χ. Then the map $\det(\chi) : G \to \mathbb{C}$ defined by

$$\det(\chi)(g) = \det(\mathcal{X}(g))$$

for every $g \in G$ is a group homomorphism (i. e. a linear character of G), and it only depends on the similarity class of $\mathcal{X}$. The multiplicative order of $\det(\chi)$ in the group of linear characters of G is the **determinantal order** of χ, and it is usually denoted by $o(\chi)$.

Two essential features in character theory are restriction and induction of characters. If φ is a class function of G and H is a subgroup of G, then the restricted function

$$\varphi_H : H \longrightarrow \mathbb{C}$$

is defined in the obvious way. Of course, the restriction of a class function of G to H is a class function of H, and the restriction of a character is a character (to prove this last assertion, restrict the representation affording the character to H).

Suppose now that θ is a class function of H; then the induced class function θ^G is defined by

$$\theta^G(g) = \frac{1}{|H|}\sum_{x \in G} \theta^0(xgx^{-1})\,,$$

where $\theta^0(h) = \theta(h)$ if $h \in H$ and $\theta^0(y) = 0$ if $y \notin H$. Frobenius reciprocity relates induction and restriction of class functions, establishing that

$$[\varphi_H, \theta] = [\varphi, \theta^G]$$

with the same notation as before (see Lemma 5.2 of [13]). In particular, characters of a subgroup induce to characters of the whole group, by Corollary 5.3 of [13]. We shall also use this without explicit mention.

1.2 Characters and normal subgroups

Let N be a normal subgroup of G and let $\hat{\chi}$ be a character of G/N. Then the function defined by

$$\chi(g) = \hat{\chi}(gN)$$

for $g \in G$ is a character of G. Conversely, if φ is a character of G containing N in its kernel, then φ is constant on the cosets of N in G, and the function

$$\hat{\varphi} : G/N \longrightarrow \mathbb{C}$$

defined by $\hat{\varphi}(gN) = \varphi(g)$, for every $g \in G$, is a character of G/N. Furthermore, φ is irreducible if and only $\hat{\varphi}$ is irreducible, and the same happens with χ and $\hat{\chi}$ (see Lemma 2.22 of [13].) It is now clear that we can identify the irreducible characters of G/N with the irreducible characters of G that contain the subgroup N in the kernel.

We also mention that, under the identification above, the linear characters of a group G are precisely the characters of G/G', where G' is the derived subgroup of G, by Corollary 2.23 of [13]. Therefore we have that if χ is a character of G then

$$\det(\chi) : G/G' \longrightarrow \mathbb{C}^\times$$

is a group homomorphism, where $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. In particular $o(\chi)$ divides $|G : G'|$.

We recall that if $N \lhd G$, then conjugation defines a natural action of G on $\mathrm{Irr}(N)$. More precisely, for $\theta \in \mathrm{Irr}(N)$ and $x \in G$, define

$$\theta^x(n) = \theta(xnx^{-1}). \tag{1.2}$$

It is then easy to check that $\theta^x \in \mathrm{Irr}(N)$. The stabilizer of θ in G under this action is the inertia group of θ in G, and it is usually denoted by $I_G(\theta)$. Note that $N \leq I_G(\theta) \leq G$.

Restriction and induction of characters have a good behavior with normal subgroups, as we next see.

Theorem 1.7 (Clifford). *Let $N \lhd G$ and let $\chi \in \mathrm{Irr}(G)$. Let θ be an irreducible constituent of χ_N and suppose $\theta = \theta_1, \theta_2, \ldots, \theta_t$ are the distinct conjugates of θ in G. Then*

$$\chi_N = e \sum_{i=1}^{t} \theta_i,$$

where $e = [\chi_N, \theta]$.

Proof. See Theorem 6.2 of [13]. ▮

If $N \lhd G$, $\theta \in \mathrm{Irr}(N)$ and $\chi \in \mathrm{Irr}(G)$ is such that $[\chi_N, \theta] \neq 0$, then we say that χ **lies over** θ, or equivalently that θ **lies under** χ. The set of irreducible characters of G lying over θ is denoted by $\mathrm{Irr}(G|\theta)$.

In the above formula

$$\chi_N = e \sum_{i=1}^{t} \theta_i ,$$

it is clear that $t = |G : I_G(\theta)|$, the index of the inertia group of θ in G. In particular, we have that t divides $|G/N|$. In fact, using the same notation, it is possible to prove that:

Theorem 1.8. *The integer $\chi(1)/\theta(1)$ divides $|G/N|$.*

Proof. See Theorem 11.29 of [13]. ▮

It then follows that $[\theta^G, \chi] = [\theta, \chi_N] = e$ divides $|G : N|$, by the Frobenius reciprocity.

The following result is fundamental.

Theorem 1.9 (Clifford's Correspondence). *Let $N \lhd G$, $\theta \in \mathrm{Irr}(N)$, and $T = I_G(\theta)$. Then*

1. *If $\psi \in \mathrm{Irr}(T|\theta)$, then ψ^G is irreducible.*
2. *The map $\psi \mapsto \psi^G$ is a bijection of $\mathrm{Irr}(T|\theta)$ onto $\mathrm{Irr}(G|\theta)$.*
3. *If $\psi^G = \chi$ with $\psi \in \mathrm{Irr}(T|\theta)$, then ψ is the unique irreducible constituent of χ_T which lies in $\mathrm{Irr}(T|\theta)$.*
4. *If $\psi^G = \chi$, with $\psi \in \mathrm{Irr}(T|\theta)$, then $[\psi_N, \theta] = [\chi_N, \theta]$.*

Proof. See Theorem 6.11 of [13]. ▮

If H is a subgroup of G and ψ is a character of H, then it is said that ψ **extends** to G if there exists a character χ of G such that $\chi_H = \psi$. Observe that if H is normal in G and ψ extends to G, then ψ is invariant in G.

Another basic result that we shall use frequently is Gallagher's theorem.

Theorem 1.10 (Gallagher). *Let $N \lhd G$ and let $\chi \in \mathrm{Irr}(G)$ be such that $\chi_N = \theta \in \mathrm{Irr}(N)$. Then the map*

$$\begin{array}{ccc} \mathrm{Irr}(G/N) & \longrightarrow & \mathrm{Irr}(G|\theta) \\ \beta & \mapsto & \beta\chi \end{array}$$

is a bijection.

Proof. See Theorem 6.17 of [13]. ▌

With the same notation as in Theorem 1.10, we remark that the set of extensions of χ_N to G is

$$\{\beta\chi \,|\, \beta \in \mathrm{Irr}(G/N) \text{ is linear}\}.$$

Under certain hypothesis, it is possible to guarantee that a character of a normal subgroup extends to the whole group. The following is a very useful result.

Theorem 1.11. *Let $N \lhd G$ and $\theta \in \mathrm{Irr}(N)$ with θ invariant in G, and suppose that $(|G:N|, \theta(1)o(\theta)) = 1$. Then θ has a unique extension $\chi \in \mathrm{Irr}(G)$ with $(|G:N|, o(\chi)) = 1$. In fact, $o(\chi) = o(\theta)$.*

Proof. See Corollary 8.16 of [13]. ▌

The character χ in Theorem 1.11 is usually referred as the **canonical extension** of θ to G. Observe that if $(|G:N|, |N|) = 1$ in the statement of the previous theorem, then θ has a canonical extension to G, by Theorem 1.4 and the comments at the beginning of this section. As we shall see, canonical extensions behave well with respect to fields of values.

1.3 Actions on characters and conjugacy classes

Suppose that G is a finite group and let $\mathrm{Cl}(G)$ be the set of conjugacy classes of G. If g is an element of G, then we write $\mathrm{Cl}_G(g)$ for the conjugacy class of g in G.

Let $A = \mathrm{Aut}(G)$ be the group of automorphisms of G, and write g^a for the image of an element $g \in G$ under the action of the automorphism $a \in A$. Observe that A acts naturally on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ via

$$\chi^a(g) = \chi(g^{a^{-1}})$$

and

$$\mathrm{Cl}_G(g)^a = \mathrm{Cl}_G(g^a),$$

where $\chi \in \mathrm{Irr}(G)$, $g \in G$ and $a \in A$. Of course, when $N \lhd G$ the action of G on N by conjugation is a particular case of this.

These actions of $\mathrm{Aut}(G)$ on the sets $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ are closely related. The following is an important result by R. Brauer.

Theorem 1.12 (Brauer's Permutation Lemma). *Let A be a group which acts on $\mathrm{Irr}(G)$ and on $\mathrm{Cl}(G)$, where G is a finite group. Assume that*

$$\chi(g) = \chi^a(g^a)$$

for all $\chi \in \mathrm{Irr}(G)$, $a \in A$ and $g \in G$, where g^a is an element of $\mathrm{Cl}_G(g)^a$. Then for each $a \in A$, the number of fixed irreducible characters of G is equal to the number of fixed conjugacy classes.

Proof. See Theorem 6.32 of [13]. ▮

We recall that if a group G acts on the non-empty sets Ω and Δ, then the two actions are called **permutation isomorphic** if there exists a bijection

$$\rho : \Omega \longrightarrow \Delta$$

such that $\rho(x \cdot g) = \rho(x) \cdot g$ for all $x \in \Omega$ and all $g \in G$, where $\cdot$ denotes the action of G on both sets.

It is important to note that the actions of $\mathrm{Aut}(G)$ on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ are not permutation isomorphic in general (we shall give examples in subsequent chapters).

Lemma 1.13. *Let G be a group acting on the sets Ω and Δ. Suppose that for every subgroup $H \leq G$, the number of fixed points of H on Ω equals the number on Δ. Then Ω and Δ are permutation isomorphic*

Proof. See Lemma 13.23 of [13]. ▮

It is clear from last result that if a cyclic group A acts on the sets $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$, where G is a finite group, and the two actions satisfy the compatibility condition in Brauer's Theorem 1.12, then the actions are permutation isomorphic.

When a group A acts coprimely on a group G via automorphisms, we have the following important natural bijection.

Theorem 1.14 (Glauberman-Isaacs Correspondence). *Let A act on a group G via automorphism, and assume that $(|A|, |G|) = 1$. Then there exists a natural correspondence*

$$\mathrm{Irr}_A(G) \longrightarrow \mathrm{Irr}(\mathbf{C}_G(A)),$$

where $\mathrm{Irr}_A(G)$ is the set of A-invariant irreducible characters of G and $\mathbf{C}_G(A)$ is the subgroup of A-invariant elements of G.

Proof. See Theorem 10.8 of [17] and Theorem 13.1 of [13]. ▮

The word "natural" in the previous statement means that there is an algorithm to construct the correspondence, and the possible choices made in the construction of the correspondence do not change the final result.

1.4 Galois action and rationality

Let n be any positive integer and $\xi \in \mathbb{C}$ a primitive nth root of unity. We denote by $\mathbb{Q}_n = \mathbb{Q}(\xi)$ the nth cyclotomic extension over the field of rational numbers and we write

$$\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$$

for the Galois group of this extension. Observe that if $\sigma \in \mathcal{G}_n$ then ξ^σ is also a primitive nth root of unity and therefore

$$\xi^\sigma = \xi^t$$

for an integer t coprime to n and unique modulo n. It is also clear that t does not depend on the choice of ξ. By basic field theory, we have that t determines the automorphism σ and we can then write $\sigma = \sigma_t$. In other words, we have that

$$\begin{array}{ccc} \mathcal{G}_n & \longrightarrow & \mathrm{Aut}(\langle\xi\rangle) \\ \sigma & \mapsto & f \end{array} \tag{1.3}$$

is a well-defined, injective group homomorphism, where $f(\xi) = \xi^t$ provided that $\sigma = \sigma_t$.

Conversely, for every integer $1 \leq t \leq n$ coprime to n, there exists $\sigma \in \mathcal{G}_n$ such that $\sigma = \sigma_t$. In order to see this, recall that $\mathcal{G}_n$ has size $\Phi(n)$, where Φ is the Euler function, by basic Galois theory. In particular, the map 1.3 is a group isomorphism.

Suppose that G is a finite group and let n be a multiple of the exponent of G. Then the Galois group $\mathcal{G}_n$ acts naturally on the set of conjugacy classes of G via

$$\mathrm{Cl}_G(g)^{\sigma_t} = \mathrm{Cl}_G(g^t)\,, \tag{1.4}$$

where $g \in G$ and $\sigma_t \in \mathcal{G}_n$. It is routine to check that this is a well-defined action, using the fact that t is coprime to the exponent of G.

If $\chi \in \mathrm{Irr}(G)$ and $g \in G$, it is a basic fact that there exists a representation $\mathcal{Y}$ of G affording χ such that

$$\mathcal{Y}(g) = \mathrm{diag}(\epsilon_1, \ldots, \epsilon_f)\,, \tag{1.5}$$

where each ϵ_i is a complex root of unity of order a divisor of the order of g and $\chi(1) = f$. In particular, all values of χ lie in $\mathbb{Q}_n$.

It is not difficult to show that every ordinary character $\chi \in \mathrm{Irr}(G)$ is afforded by a representation of G with entries on the field of algebraic numbers in $\mathbb{C}$ (see page 22 of [13]). Therefore, χ is in fact afforded by a representation over a finite degree Galois extension E of $\mathbb{Q}$, and we can assume that E contains the cyclotomic extension $\mathbb{Q}_n$. Let $\sigma \in \mathcal{G}_n$ and

$$\mathcal{X} : G \longrightarrow \mathrm{GL}(f, E)$$

be a representation affording $\chi \in \mathrm{Irr}(G)$. By elementary field theory, we can extend σ to an automorphism $\hat{\sigma}$ of E. Then we can apply $\hat{\sigma}$ to the entries of the matrix $\mathcal{X}(g)$, where $g \in G$, and we obtain a new matrix in $\mathrm{GL}(f, E)$. In fact, it is easy to see that if we do this for every $g \in G$, we get another irreducible E-representation of G which is denoted by $\mathcal{X}^{\hat{\sigma}}$. Clearly, $\mathcal{X}^{\hat{\sigma}}$ affords the complex character

$$\chi^\sigma(g) = \chi(g)^\sigma, \tag{1.6}$$

where $g \in G$. Note that χ^σ is indeed determined by σ, and $\chi^\sigma \in \mathrm{Irr}(G)$. It is now clear that $\mathcal{G}_n$ acts naturally on $\mathrm{Irr}(G)$ via 1.6. Furthermore, by Theorem 1.2 it follows that this also induces an action of $\mathcal{G}_n$ on the set of (possibly reducible) characters of G.

Note that since the exponent of a finite group G divides the order $|G| = k$, the Galois group $\mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q})$ acts naturally on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$.

As before, suppose that G is a group of exponent a divisor of the positive integer n. Using 1.5, we have that for any $\sigma_t \in \mathcal{G}_n$ as before

$$\chi^{\sigma_t}(g) = \epsilon_1^{\sigma_t} + \cdots + \epsilon_f^{\sigma_t} = \chi(g^t)\,. \tag{1.7}$$

We remark that using the expression 1.7 and the fact that 1.3 is a group isomorphism, it is easy to see that an element $g \in G$ is conjugate to every generator of $\langle g \rangle$ in G, precisely when $\chi(g)$ is a rational number for all $\chi \in \mathrm{Irr}(G)$, applying Theorem 1.2. In this case g is a **rational** element of G, and it is now clear that the conjugacy classes containing rational elements, i. e. the **rational classes**, are just those classes of G fixed by the action of $\mathcal{G}_n$. The set of rational conjugacy classes of G is denoted by $\mathrm{Cl}_{\mathbb{Q}}(G)$.

A character χ of G is called **rational** if $\chi(g) \in \mathbb{Q}$ for all $g \in G$, and it is clear from Galois theory that the rational irreducible characters of G are exactly those characters in $\mathrm{Irr}(G)$ fixed by the group $\mathcal{G}_n$ in the natural action. We write $\mathrm{Irr}_{\mathbb{Q}}(G)$ for the set of irreducible rational characters of G.

Similarly, a character χ of G is **real** if $\chi(g)$ is a real number for all $g \in G$, and an element $g \in G$ is **real** if $\chi(g) \in \mathbb{R}$ for every $\chi \in \mathrm{Irr}(G)$. Observe that by 1.5, we have that

$$\chi(g^{-1}) = \overline{\chi(g)}$$

for all $\chi \in \mathrm{Irr}(G)$ and $g \in G$. Using the Second Orthogonality Relation, it is now easy to see that $g \in G$ is real if and only of g is conjugate to g^{-1} in G.

The natural actions of $\mathcal{G}_n$ on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ satisfy the compatibility condition in Brauer's Theorem 1.12. To see this, we need to modify slightly the action of $\mathcal{G}_n$ on the set of classes by setting

$$\mathrm{Cl}_G(g)^{\sigma_t} = \mathrm{Cl}_G(g^s)\,,$$

where $\sigma_t \in \mathcal{G}_n$, $g \in G$ and $ts \equiv 1 \pmod{n}$ with $1 \leq s \leq n$. Note that $\sigma_s = (\sigma_t)^{-1}$ and consequently the conjugacy classes fixed by σ_t and σ_s in 1.4 are exactly the same.

Let G be a finite group of exponent n. Complex conjugation induces a Galois automorphism on $\mathbb{Q}_n$, and therefore it permutes the sets $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$. By Brauer's Permutation Lemma, the number of irreducible characters of G fixed by complex conjugation is equal to the number of fixed conjugacy classes, so the number of real-valued irreducible characters of G equals the number real conjugacy classes of G.

It is immediate to check that Galois action on characters and conjugacy classes commutes with action induced by group automorphisms.

1.5 Basic π-theory

Fix a set π of primes numbers, and recall that if n is a positive integer then the **π-part** of n is the greatest integer n_π whose prime factors lie in π and

$$n_\pi \,|\, n\,.$$

Also, n is called is a π-**number** if $n_\pi = n$. As it is customary, we denote by π' the complement of π in the set of prime numbers; if the set π consists of a single prime p, then it is often written $\pi = p$ and $\pi' = p'$.

An element g in a finite group G is a called a π-**element** if it has order $o(g)$ a π-number, and a group G is a π-**group** if its order $|G|$ is a π-number. It is an elementary fact that every element g in a finite group G can be uniquely decomposed as a product

$$g = uv$$

with u, v powers of g, u a π-element and v a π'-element. The element u is called the π-**part** of g.

A finite group G is π-**separable** if there exists a series of normal subgroups $N_i \trianglelefteq G$ of the form

$$1 = N_0 \leq N_1 \leq \cdots \leq N_i \leq \cdots \leq N_r = G$$

and such that each factor N_i/N_{i-1} is either a π-group or a π'-group, for $1 \leq i \leq r$. If in addition each π-factor of the series is solvable then G is called π-**solvable**. Note that if p is a prime, then each p-separable group is p-solvable, and we usually refer to a p-separable group as a p-solvable group. We also recall that a finite solvable group G is π-separable for every set of primes π (see Corollary 3.19 of [14]).

Now let G be a finite π-separable group. In the important paper [16], M. Isaacs defined a canonical subset $B_\pi(G)$ of the complex irreducible characters $\mathrm{Irr}(G)$. Probably, the main property of this set is that $B_{p'}$-characters constitute a lifting of the irreducible Brauer characters of a p-solvable group G at the prime p, that is restriction to p-regular elements (elements of order coprime to p) defines a bijection $B_{p'}(G) \to \mathrm{IBr}(G)$, where $\mathrm{IBr}(G)$ is the set of Brauer characters of G at p. We shall not need this lifting, but we shall use other properties of B_π-characters, since they are a powerful tool in the character theory of π-separable groups.

It easily follows from the definition of the B_π-characters that the principal character is always a π-character, and if G is a π-group then $B_\pi(G) = \mathrm{Irr}(G)$.

The characters in B_π are closed under group automorphisms and Galois action.

Theorem 1.15. *Let $\chi \in B_\pi(G)$, $a \in \mathrm{Aut}(G)$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$. Then both characters χ^a and χ^σ lie in $B_\pi(G)$.*

Proof. See of [16]. ∎

Another remarkable fact is that the values of B_π-characters lie in cyclotomic extensions of the rationals by roots of order a π-number. Recall that $\mathbf{O}_\pi(G)$ is the maximal normal π-subgroup of a group G.

Theorem 1.16. *Let $\chi \in B_\pi(G)$ and write $|G|_\pi = m$. Then $\chi(g) \in \mathbb{Q}_m$ for all $g \in G$ and $\mathbf{O}_{\pi'}(G) \leq \ker(\chi)$.*

Proof. See Corollaries 5.3 and 12.1 of [16]. ▮

The following is a deep fact on B_π-characters.

Theorem 1.17. *The number of conjugacy classes of G consisting of π-elements equals the number of characters in $B_\pi(G)$. Furthermore, the square matrix*

$$A = (\chi(x)),$$

where $\chi \in B_\pi(G)$ and x runs over representatives of the conjugacy classes of π-elements of G, is invertible.

Proof. See Corollary 10.2 of [16]. ▮

As a consequence of last result and Theorem 1.15, it is possible to prove the following version of Brauer's Permutation Lemma for B_π-characters and conjugacy classes of π-elements.

Theorem 1.18. *Let A be a group which acts on $\mathrm{Irr}(G)$ and on $\mathrm{Cl}(G)$, where G is a finite π-solvable group. Assume that either the action is induced by automorphisms of G, or it is a Galois action. Then for each $a \in A$, the number of fixed B_π-characters of G is equal to the number of fixed conjugacy classes of π-elements of G.*

Proof. The proof of Brauer's Permutation Lemma works in this case aswell, since the matrix considered in Theorem 1.17 is invertible, and both $B_\pi(G)$ and the set of conjugacy classes of π-elements of G are invariant under the action of A. ▮

Let us also collect some results about B_π-characters and normal subgroups.

Theorem 1.19. *Suppose that $N \lhd G$ and G/N is a π-group. If $\psi \in B_\pi(N)$, then $\mathrm{Irr}(G|\psi) \subseteq B_\pi(G)$.*

Proof. See Theorem 7.1 of [16]. ▮

On the other hand:

Theorem 1.20. *Let $N \lhd G$ with G/N a π'-group and $\psi \in B_\pi(N)$. Then there exists a unique B_π-character $\chi \in \mathrm{Irr}(G|\psi)$. Furthermore, if ψ is invariant in G then ψ has a unique B_π-extension to G.*

Proof. See Theorem 6.2 and Corollary 6.3 of [16]. ▮

The key fact on restriction of B_π-characters to normal subgroups is given in the following result.

Theorem 1.21. *Let $\chi \in B_\pi(G)$ and $N \lhd G$. Then every irreducible constituent of χ_N is a B_π-character of N.*

Proof. See Corollary 7.5 of [16]. ▮

In general, it is not an easy task to recognize B_π-characters, since their definition is quite technical. Fortunately, in groups of odd order there is an easier method.

Theorem 1.22. *Let τ be the complex Galois automorphism fixing π-power roots of unity and complex-conjugating π'-roots of unity. If G has odd order and $\chi \in \mathrm{Irr}(G)$, then $\chi \in B_\pi(G)$ if and only if $\chi^\tau = \chi$.*

Proof. This is Lemma (3.1) of [15]. ▮

Chapter 2

Rationality and Sylow 2-subgroups

2.1 Introduction

Rationality questions in a finite group G are believed to be somehow related to the Sylow 2-subgroups of G, the first reason being, perhaps, that groups of odd order do not possess non-trivial rational irreducible characters nor classes (this follows from a well-known theorem of Burnside, see Section 3.2). For instance, it was a long open problem to determine whether a Sylow 2-subgroup of a rational group is itself rational. However, a negative answer to this question was recently given in [19].

It is convenient to recall that it is not true that the natural actions of the Galois group $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ on $\mathrm{Irr}(G)$ and on the set of classes $\mathrm{Cl}(G)$ of a group G are permutation isomorphic, where n is the exponent of G and $\mathbb{Q}_n$ is the nth cyclotomic field (see Section 1.4). Whenever these actions are permutation isomorphic, of course we have that $|\mathrm{Irr}_{\mathbb{Q}}(G)| = |\mathrm{Cl}_{\mathbb{Q}}(G)|$, because the rational characters are precisely the $\mathcal{G}_n$-invariant characters, and the same happens with the rational conjugacy classes.

We mention that if the actions of $\mathcal{G}_n$ on the set $\mathrm{Irr}(G)$ and on $\mathrm{Cl}(G)$ are isomorphic, then in fact there is a bijection between $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ preserving fields of values (the field of values of $\chi \in \mathrm{Irr}(G)$ is the smallest field containing the values of χ, and similarly for $C \in \mathrm{Cl}(G)$, see Section 2.2 below). It is important to remark that a group G may satisfy that $|\mathrm{Irr}_{\mathbb{Q}}(G)| = |\mathrm{Cl}_{\mathbb{Q}}(G)|$ and yet the $\mathcal{G}_n$-actions on classes and characters not be isomorphic, as examples of odd-order groups illustrate.

The smallest example of a group G with different number of rational classes than rational irreducible characters is the group of order 2^5 defined by the generators and relators

$$G = \langle a, b, c \mid a^2 = b^2 = c^8 = 1, [a, b] = [b, c] = 1, c^a = bc^3 \rangle,$$

which has 6 irreducible rational characters and 8 rational conjugacy classes. Let us consider more examples of this type that will appear later. Suppose that G is a group generated by elements a and b, where $o(a) = m$ and $o(b) = n$ are both powers of 2 bigger than 4. Assume that $a^b = a^k$, with $k \equiv -1 \pmod 4$, $k^{m/4} \equiv 1 \pmod n$ and $a^{n/2} = b^{m/2}$. We shall see in Chapter 4 that such a group G has four rational conjugacy classes, and it is not difficult to check that $|\mathrm{Irr}_{\mathbb{Q}}(G)| = 6$.

It follows from the main result of [2] that $|\mathrm{Irr}_{\mathbf{Q}}(G)| = |\mathrm{Cl}_{\mathbf{Q}}(G)|$ if all Sylow subgroups of G are abelian, since under this hypothesis Galois actions on classes and irreducible characters are isomorphic. General results guaranteeing that $|\mathrm{Irr}_{\mathbf{Q}}(G)| = |\mathrm{Cl}_{\mathbf{Q}}(G)|$ are rare in the literature; we mention that another result of this type can be found in [31]. In this chapter we count rational characters and rational classes of certain groups. In particular, we can prove the following, which is the main result in the chapter and has been published in a joint work of the author and G. Navarro [30].

Theorem A. *Suppose that $P \in \mathrm{Syl}_2(G)$ is cyclic. Then $|\mathrm{Irr}_{\mathbf{Q}}(G)| = |\mathrm{Cl}_{\mathbf{Q}}(G)|$.*

Even the case where $|P| = 2$ in Theorem A is non-trivial and relies on the recent paper [28] on quadratic characters of groups of odd order, as we shall explain. Our methods here are in fact slightly more general and apply, for instance, to analyze when groups with a normal Sylow p-subgroup G have the same number of rational classes as rational irreducible characters, as we shall see in the last section of the chapter.

Unfortunately, Theorem A does not seem to open a variety of results of similar type: if we change cyclic to $C_2 \times C_2$, Theorem A is already false, even assuming that G has a normal 2-complement. Particularly, Example 2.21 below shows that there exists a group of order $2^2 \cdot 3^4 \cdot 7$ having an elementary abelian Sylow 2-subgroup P, a normal 2-complement and different number of rational characters and rational classes. The same happens if P is quaternion or dihedral of order 8, as we indicate in the last last section of this chapter.

We observe that it is not true that in a group G with a cyclic Sylow 2-subgroup the actions of $\mathcal{G}_n$ on $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ are isomorphic, since there are odd-order groups with non-isomorphic Galois actions.

2.2 Preliminary Results

As is well-known, the groups in Theorem A have a normal 2-complement.

Theorem 2.1. *Let G be a finite group, and assume that G has a cyclic Sylow 2-subgroup. Then G has a normal 2-complement.*

Proof. See Theorem 5.14 of [14]. ∎

We start by presenting some general facts on rationality and normal subgroups. First we treat characters and later on, we give a description of the rational conjugacy classes of a group having a normal p-complement.

2.2.1 Characters

Suppose that G is a finite group and χ is a possibly reducible character of G. Then the **field of values** of χ in G is the smallest complex field containing all values of χ in G, and we denote it by

$$\mathbb{Q}(\chi) = \mathbb{Q}(\chi(g) \mid g \in G).$$

Of course, we have that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}_n$, where n is the exponent of G. By Section 1.4, the Galois group $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ acts naturally on the set of characters of G via

$$\chi^\sigma(g) = (\chi(g))^\sigma,$$

for $\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ and $g \in G$. In particular, a character χ of G is σ-invariant if and only if

$$\sigma \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(\chi)),$$

and we deduce by Galois theory that the $\mathcal{G}_n$-orbit of χ has size

$$|\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) : \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(\chi))| = |\mathbb{Q}(\chi) : \mathbb{Q}|.$$

Let us recall the following elementary fact, which we shall use frequently.

Lemma 2.2. *Suppose that $F/\mathbb{Q}$ is a finite complex extension of the field of rational numbers. Let $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ and suppose that χ is a character of G such that $\mathbb{Q}(\chi) \subseteq F$. Then the map χ^σ defined by the expression*

$$\chi^\sigma(x) = \chi(x)^\sigma,$$

where $x \in G$, is a character of G. Furthermore, $\chi \in \mathrm{Irr}(G)$ if and only if $\chi^\sigma \in \mathrm{Irr}(G)$.

Proof. We know from the comments in Section 1.4 that χ is afforded by an E-representation $\mathcal{X}$ of G, where E is some finite Galois extension of the rational numbers, which can be taken with $F \subseteq E$. Let $\hat{\sigma}$ be an extension of σ to E. As in Section 1.4, write $\mathcal{X}^{\hat{\sigma}}$ for the (complex) representation obtained by applying $\hat{\sigma}$ to each entry of the matriecs in the image of $\mathcal{X}$, so we have that $\mathcal{X}^{\hat{\sigma}}$ affords the ordinary character χ^σ, and the first part of the result is proved. The last part can be easily checked by using the orthogonality relations. ∎

In particular, it is clear from Lemma 2.2 that if χ is a character of G and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\chi)/\mathbb{Q})$, then χ^σ is also a character of G.

When dealing with fields of values of characters and normal subgroups, it is sometimes convenient to use the so-called **semi-inertia** subgroup. Suppose that N is a normal subgroup of the group G and let $\theta \in \mathrm{Irr}(N)$. If g is an element of G, then we have that $\mathbb{Q}(\theta) = \mathbb{Q}(\theta^g)$, as it is immediate to check. Let $T = I_G(\theta)$ be the inertia group of θ in G, and define the semi-inertia group of θ in G as

$$T^* = \left\{ g \in G \,\middle|\, \theta^g = \theta^\sigma \text{ for some } \sigma \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}) \right\}.$$

In order to check that T^* is actually a subgroup of G, suppose that $g, h \in T^*$ and let $\sigma, \tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ with $\theta^\sigma = \theta^g$ and $\theta^\tau = \theta^h$. Then

$$\theta^{gh} = (\theta^\sigma)^h = (\theta^h)^\sigma = \theta^{\tau\sigma},$$

because Galois automorphisms commute with conjugation of G on $\mathrm{Irr}(N)$. Also note that since $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ is abelian then $(T^*)' \leq T$.

Lemma 2.3. *Let $N \lhd G$ and $\theta \in \mathrm{Irr}(N)$. Also, write T and T^* be as before.*

1. *Suppose that* $\chi \in \mathrm{Irr}(G|\theta)$ *and assume that* $\mathbb{Q}(\chi), \mathbb{Q}(\theta) \subseteq F$, *where* $F/\mathbb{Q}$ *is a finite abelian Galois extension. If* $\sigma \in \mathrm{Gal}(F/\mathbb{Q}(\chi))$, *then there exists* $g \in T^*$ *such that* $\theta^g = \theta^\sigma$.

2. *If* $\psi \in \mathrm{Irr}(T|\theta)$, *then* $\mathbb{Q}(\psi^{T^*}) = \mathbb{Q}(\psi^G)$.

Proof. By Lemma 2.2, we have that $\theta^\sigma \in \mathrm{Irr}(N)$. Now, it is clear from the definition of the inner product that

$$[(\chi^\sigma)_N, \theta^\sigma] = [\chi_N, \theta]$$

and we see that θ^σ lies under $\chi^\sigma = \chi$. Hence $\theta^\sigma = \theta^g$ for some $g \in G$ by Clifford's Theorem 1.7. As $\mathbb{Q}(\theta)/\mathbb{Q}$ is a normal extension, σ restricts to an automorphism of $\mathbb{Q}(\theta)$. Then we easily see that $g \in T^*$. This proves part 1.

To prove part 2, write $\eta = \psi^{T^*} \in \mathrm{Irr}(T^*|\theta)$ and $\chi = \psi^G \in \mathrm{Irr}(G|\theta)$. Since $\eta^G = \chi$, we have that

$$\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\eta) \subseteq \mathbb{Q}(\psi)$$

by the induction formula. It suffices to show that if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\chi))$ then $\eta^\sigma = \eta$. Since $\psi_N = e\theta$, we have that $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\psi)$. By part 1 taking $F = \mathbb{Q}(\psi)$, we have that $\theta^\sigma = \theta^g$ for some $g \in T^*$. Now $(\psi^\sigma)^{g^{-1}}$ lies over θ and induces χ, so

$$(\psi^\sigma)^{g^{-1}} = \psi$$

by the uniqueness in the Clifford correspondence. Thus $\psi^\sigma = \psi^g$ and

$$\eta^\sigma = (\psi^\sigma)^{T^*} = (\psi^g)^{T^*} = \psi^{T^*} = \eta\,,$$

as desired. ∎

We shall use the following elementary lemma several times. The first part is Lemma 2.2 of [21], but we include a proof for the reader's convenience.

Lemma 2.4. *Let* $N \lhd G$, $\theta \in \mathrm{Irr}(N)$, T *and* T^* *be as before. Then the map*

$$T^* \longrightarrow \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$$

given by $g \mapsto \sigma$ *and defined by the equation* $\theta^g = \theta^\sigma$ *is a well-defined group homomorphism with kernel* T *and image* $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G))$. *In particular, we have that* θ^G *is rational valued if and only if*

$$|T^*/T| = |\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})|\,.$$

This happens, for instance, if there exists some $\chi \in \mathrm{Irr}(G|\theta)$ *rational valued.*

Proof. The map in the statement is easily seen to be a group homomorphism, using that $(\theta^x)^\sigma = (\theta^\sigma)^x$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ and $x \in G$, and that $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ is abelian. Of course, T is the kernel of this homomorphism.

Suppose now that $\theta^g = \theta^\sigma$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ and $g \in G$. Then

$$(\theta^G)^\sigma = (\theta^\sigma)^G = (\theta^g)^G = \theta^G,$$

so $\sigma \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G))$. Also, for any $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G))$ we have that τ permutes the irreducible constituents of $(\theta^G)_N$. These constituents are the G-conjugates of θ, and we deduce that $\theta^\tau = \theta^y$ for some $y \in T^*$. Thus, the map has image $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G))$.

Assume now that there exists $\chi \in \mathrm{Irr}(G|\theta)$ which is rational valued. Since θ^G is zero off N and $(\theta^G)_N$ is a rational multiple of χ_N, we see that $\mathbb{Q}(\theta^G) = \mathbb{Q}(\chi_N)$ and the last part follows. ∎

Hence, we see that there exists a natural isomorphism

$$\rho_\theta = \rho : \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G)) \longrightarrow T^*/T. \tag{2.1}$$

If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G))$, then $\rho(\sigma)$ is the unique (modulo T) element in T^* such that

$$\theta^\sigma = \theta^{\rho(\sigma)}.$$

Theorem 2.5. *Let $N \lhd G$, $\theta \in \mathrm{Irr}(N)$, T and T^* be as before, and suppose that θ^G is rational valued.*

1. *Let $\psi \in \mathrm{Irr}(T|\theta)$ and $\chi = \psi^G$. Then χ is rational valued if and only if $\mathbb{Q}(\psi) = \mathbb{Q}(\theta)$ and*
$$\psi^\tau = \psi^{\rho(\tau)}$$
for all $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$.

2. *Let $\psi \in \mathrm{Irr}(T|\theta)$ be such that ψ^G is rational valued, and assume that $\psi_N = \theta$. Let $\epsilon \in \mathrm{Irr}(T/N)$. Then $(\epsilon\psi)^G$ is rational if and only if $\mathbb{Q}(\epsilon) \subseteq \mathbb{Q}(\theta)$ and $\epsilon^\tau = \epsilon^{\rho(\tau)}$ for all $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$.*

Proof. By hypothesis, we have a natural isomorphism $\rho : \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}) \to T^*/T$.

First we prove part 1. Suppose first that $\mathbb{Q}(\psi) = \mathbb{Q}(\theta)$ and $\psi^\tau = \psi^{\rho(\tau)}$ for all $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$. We have that $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\psi) = \mathbb{Q}(\theta)$. Take $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ and write $\rho(\tau) = gT \in T^*/T$. Then

$$\chi^\tau = (\psi^G)^\tau = (\psi^\tau)^G = (\psi^g)^G = \chi$$

and we conclude that χ is rational valued.

Conversely, suppose that χ is rational valued. Since $\psi_N = e\theta$, we have that $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\psi)$. Now, take $\sigma \in \mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\theta))$ and note that $\psi^\sigma \in \mathrm{Irr}(T|\theta)$. Since χ is rational,

$$(\psi^\sigma)^G = (\psi^G)^\sigma = \chi^\sigma = \chi = \psi^G,$$

and by the uniqueness in the Clifford correspondence we deduce that $\psi^\sigma = \psi$. Hence σ is the identity in $\mathrm{Gal}(\mathbb{Q}(\psi)/\mathbb{Q}(\theta))$, and we conclude that $\mathbb{Q}(\theta) = \mathbb{Q}(\psi)$.

Now take $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ and suppose that $\rho(\tau) = gT$, so $(\theta^\tau)^{g^{-1}} = \theta$. Since $\mathbb{Q}(\theta) = \mathbb{Q}(\psi)$, we have that $(\psi^\tau)^{g^{-1}} \in \mathrm{Irr}(T)$, and it is clear that this character lies over θ. Also, $(\psi^\tau)^{g^{-1}}$ induces χ, and we conclude that $\psi^\tau = \psi^g$, again by the uniqueness in the Clifford's Correspondence. This proves 1.

Now we prove part 2. By hypothesis and part 1, we have that $\mathbb{Q}(\theta) = \mathbb{Q}(\psi)$ and $\psi^\tau = \psi^{\rho(\tau)}$ for all $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$. Note that by Gallagher's Theorem 1.10, we have that $\epsilon\psi \in \mathrm{Irr}(T)$, and $(\epsilon\psi)^G$ is irreducible by Clifford's Correspondence. Suppose first that $(\epsilon\psi)^G$ is rational valued. Let F be the smallest extension containing $\mathbb{Q}(\epsilon)$ and $\mathbb{Q}(\theta)$. Of course, $F/\mathbb{Q}$ is finite and we can use Lemma 2.2. Let $\tau \in \mathrm{Gal}(F/\mathbb{Q}(\theta))$. Since τ fixes θ, then τ fixes ψ, because $\mathbb{Q}(\theta) = \mathbb{Q}(\psi)$. Now $(\epsilon\psi)^\tau$ induces $(\epsilon\psi)^G$ and lies over θ. By the uniqueness in the Clifford's Correspondence, we deduce that $(\epsilon\psi)^\tau = \epsilon\psi$. Now

$$\epsilon\psi = (\epsilon\psi)^\tau = \epsilon^\tau\psi^\tau = \epsilon^\tau\psi\,,$$

and we deduce that $\epsilon^\tau = \epsilon$ by the uniqueness in Gallagher's Theorem 1.10. Hence $\mathbb{Q}(\epsilon) \subseteq \mathbb{Q}(\theta)$. Now by part 1, if $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$, we have that $(\epsilon\psi)^\tau = (\epsilon\psi)^{\rho(\tau)} = \epsilon^{\rho(\tau)}\psi^{\rho(\tau)} = \epsilon^{\rho(\tau)}\psi^\tau$. But $(\epsilon\psi)^\tau = \epsilon^\tau\psi^\tau$, and we deduce that $\epsilon^\tau = \epsilon^{\rho(\tau)}$, again by uniqueness in Gallagher's result.

Conversely, if $\mathbb{Q}(\epsilon) \subseteq \mathbb{Q}(\theta)$, then

$$\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\epsilon\psi) \subseteq \mathbb{Q}(\theta)$$

(the first containment because $(\epsilon\psi)_N = \epsilon(1)\theta$ and the second because $\mathbb{Q}(\psi), \mathbb{Q}(\epsilon) \subseteq \mathbb{Q}(\theta)$). It is easy to see that $\mathbb{Q}(\epsilon\psi) = \mathbb{Q}(\theta)$, and the result easily follows from part 1. ∎

As we have seen, if N is a normal subgroup of G and $\theta \in \mathrm{Irr}(N)$ is such that θ^G is rational valued, then we have that

$$\theta^\tau = \theta^{\rho(\tau)}$$

for $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$. Notice that if there is a *canonical* choice of some $\psi \in \mathrm{Irr}(T|\theta)$, then we might easily check that $\psi^\tau = \psi^{\rho(\tau)}$ too, and then we are ready to use Theorem 2.5. For instance when $(|N|, |G:N|) = 1$ we can consider canonical extensions described in Theorem 1.11. Recall that in this situation we have that

$$(o(\theta)\theta(1), |T:N|) = 1\,,$$

and if ψ is the canonical extension of θ to T, we see that $\mathbb{Q}(\theta) = \mathbb{Q}(\psi)$. To show that this equality holds, first note that $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\psi)$, because ψ extends θ, so we only need to prove the reverse containment. Now if n is a multiple of the exponent of G, then $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(\theta))$ acts naturally on both sets $\mathrm{Irr}(T)$ and $\mathrm{Irr}(N)$. We take $\sigma \in \mathcal{G}$ and we note that $\psi^\sigma \in \mathrm{Irr}(T)$ extends θ, because θ is $\mathcal{G}$-invariant. Then, observe that $o(\psi^\sigma) = o(\psi)$, and so

$$\psi^\sigma = \psi$$

by uniqueness of the canonical extension. So it follows that $\mathbb{Q}(\psi) \subseteq \mathbb{Q}(\theta)$ by elementary Galois theory, as wanted. Finally, the fact that $\psi^\tau = \psi^g$ whenever $\theta^\tau = \theta^g$, where $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ and $g \in G$, follows exactly from the same kind arguments, since the action of G on $\mathrm{Irr}(N)$ also preserves determinantal orders of characters.

Corollary 2.6. *Let $N \lhd G$, $\theta \in \mathrm{Irr}(N)$, T and T^* be as before, and suppose that θ^G is rational valued. If $(|N|, |G/N|) = 1$, then the number of $\varphi \in \mathrm{Irr}(G|\theta)$ rational valued is the number of rational $\epsilon \in \mathrm{Irr}(T/N)$ which are T^*-invariant. In particular, this number is $|\mathrm{Irr}_{\mathbb{Q}}(T/N)|$ if T^*/N is abelian.*

Proof. Since $(|N|, |T/N|) = 1$, by Theorem 1.11, there exists a unique canonical extension $\psi \in \mathrm{Irr}(T)$ of θ such that $o(\theta) = o(\psi)$. By the comments before this corollary, $\mathbb{Q}(\psi) = \mathbb{Q}(\theta)$ and $\psi^\tau = \psi^g$ whenever $\theta^\tau = \theta^g$, for all $\tau \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ and $g \in G$. Now, by part 1 of Theorem 2.5 we see that ψ^G is rational valued. Now, note that $\epsilon \in \mathrm{Irr}(T/N)$ has values in $\mathbb{Q}(\theta) \subseteq \mathbb{Q}_{|N|}$ if and only if ϵ is rational valued by coprimeness. The result now follows from part 2 of Theorem 2.5. ∎

With the same notation as in last result, notice that if θ^G is not rational, then there are no rational characters over θ by the last part of Lemma 2.4 .

2.2.2 Conjugacy Classes

As before, suppose that G is a finite group and let $C = \mathrm{Cl}_G(x)$ be the conjugacy class of $x \in G$. The **field of values** of C in G is the minimal complex field containing all the values that characters of G take on the class C, and we denote it by

$$\mathbb{Q}(C) = \mathbb{Q}(x) = \mathbb{Q}(\chi(x) \,|\, \chi \in \mathrm{Irr}(G)) .$$

Notice that we always have that $\mathbb{Q}(C) \subseteq \mathbb{Q}_n$ if n is a multiple of the exponent of G. Let $\sigma = \sigma_t \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ be such that $\xi^{\sigma_t} = \xi^t$, for any complex primitive nth root of unity ξ and t an integer coprime to n, as in Section 1.4. Then, with the usual notation, $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ acts on the conjugacy classes of G via

$$\mathrm{Cl}_G(x)^{\sigma_t} = \mathrm{Cl}_G(x^t) .$$

We know from Section 1.4 that for any $\chi \in \mathrm{Irr}(G)$ we can write

$$\chi(x) = (\epsilon_1 + \cdots + \epsilon_f) \tag{2.2}$$

where $\epsilon_i^n = 1$. Therefore we have that

$$\chi(x)^{\sigma_t} = \chi(x^t) .$$

In particular, we observe that $\sigma_t \in \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(C))$ if and only if $\chi(x)^{\sigma_t} = \chi(x)$ for all $\chi \in \mathrm{Irr}(G)$, which is the same to say that x^t is G-conjugate to x, by Theorem 1.2, or equivalently $C^{\sigma_t} = C$. Hence, we see that the stabilizer of the conjugacy class $C = \mathrm{Cl}_G(x)$ in $\mathcal{G}_n$ is $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(C))$. Thus we deduce that the $\mathcal{G}_n$-orbit of C has size

$$|\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) : \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(C))| = |\mathbb{Q}(C) : \mathbb{Q}| ,$$

by elementary Galois theory.

From the above discussion, it is clear that fields of values of conjugacy classes are completely determined by the action of $\mathcal{G}_n$ on $\mathrm{Cl}(G)$. Since this is also the case for fields of values of irreducible characters, as we saw in 2.2.1, it is clear that if the actions of $\mathcal{G}_n$

on the sets $\mathrm{Irr}(G)$ and $\mathrm{Cl}(G)$ are permutation isomorphic, then there is a bijection from $\mathrm{Irr}(G)$ onto $\mathrm{Cl}(G)$ preserving fields of values.

We can proceed in a similar fashion as in Lemma 2.2 to demonstrate that if $C = \mathrm{Cl}_G(x)$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(C)/\mathbb{Q})$, then σ uniquely defines a conjugacy class C^σ of G. In order to see this, first note that by Galois theory we can extend σ to some $\sigma_t \in \mathcal{G}_n$, using the same notation as above. Then it is defined

$$C^\sigma = C^{\sigma_t} = \mathrm{Cl}_G(x^t)\,,$$

as in 1.4 of Section 1.4. Of course, we need to check that this is well-defined. Suppose then that $\sigma_s \in \mathcal{G}_n$ also extends σ, and observe that then we have that

$$\chi(x)^{\sigma_t} = \chi(x)^{\sigma_s}$$

for all $\chi \in \mathrm{Irr}(G)$. Hence x^t and x^s are G-conjugate, by Theorem 1.2, and so we conclude that C^σ is well-defined, as desired. We also remark that $C^\sigma = C$ if and only if $\sigma = 1$, as follows from the discussion on the previous page.

Suppose now that H is a subgroup of G and $C = \mathrm{Cl}_H(h)$ is a conjugacy class of H; then we write

$$C^G = \mathrm{Cl}_G(h)\,.$$

Notice that $\mathbb{Q}(C^G) \subseteq \mathbb{Q}(C)$ by definition of field of values. Assume now that $C = \mathrm{Cl}_N(n)$, where N is a normal subgroup of G. In a similar way to what we have for characters, we define

$$\mathbf{N}_G(C)^* = \left\{ g \in G \,\middle|\, C^g = C^\sigma \text{ for some } \sigma \in \mathrm{Gal}(\mathbb{Q}(C)/\mathbb{Q}) \right\}.$$

Observe that $\mathbf{N}_G(C)^*$ is the group formed by the elements $g \in G$ such that n^g is conjugate to some power of n in N.

Lemma 2.7. *The map*

$$\rho_C : \mathbf{N}_G(C)^* \longrightarrow \mathrm{Gal}(\mathbb{Q}(C)/\mathbb{Q}(C^G))$$

given by $g \mapsto \sigma$, defined by the equation $C^g = C^\sigma$, is an onto group homomorphism with kernel $\mathbf{N}_G(C) = \{g \in G \mid C^g = C\}$.

Proof. Suppose that $C^g = C^\sigma = \mathrm{Cl}_N(n^t)$. If $\chi \in \mathrm{Irr}(G)$, then

$$\chi(n)^\sigma = \chi(n^t) = \chi(n^g) = \chi(n)\,,$$

so we see that $\sigma \in \mathrm{Gal}(\mathbb{Q}(C)/\mathbb{Q}(C^G))$. Conversely, if $\sigma \in \mathrm{Gal}(\mathbb{Q}(C)/\mathbb{Q}(C^G))$ and σ agrees with σ_t on $\mathbb{Q}(C)$, then we have that

$$\chi(n^t) = \chi(n)^\sigma = \chi(n)$$

for all $\chi \in \mathrm{Irr}(G)$. Hence, n^t and n are G-conjugate by Theorem 1.2. So there is $g \in \mathbf{N}_G(C)^*$ such that $C^g = C^\sigma$, by definition of $\mathbf{N}_G(C)^*$.

It follows from the previous paragraph that the map ρ_C is well-defined. The fact that it is a group homomorphism can be checked by routine arguments, using that

$\mathrm{Gal}(\mathbb{Q}(C)/\mathbb{Q}(C^G))$ is abelian, and Galois action commutes with action induced by group automorphism on conjugagy classes. ▮

We shall frequently use the fact that if A acts coprimely on G , then the map

$$C \mapsto C \cap \mathbf{C}_G(A)$$

defines a bijection from the set of A-invariant conjugacy classes of G onto the set of conjugacy classes of $\mathbf{C}_G(A)$, the subgroup of fixed points of A in G. This result is Corollary 13.10 of [14].

Next, we give an appropriate set of representatives of conjugacy classes in a coprime action, which is fairly well-known.

Lemma 2.8. *Suppose that $N \lhd G$ with $(|G:N|, |N|) = 1$ and let H be a complement of N in G.*

1. *Let C be a conjugacy class of N and let*

$$\mathbf{N}_G(C) = \{x \in G \mid C^x = C\}.$$

Write $C = \mathrm{Cl}_N(n)$, where $[n, \mathbf{N}_H(C)] = 1$. Let $h_1, h_2 \in \mathbf{N}_H(C)$. Then nh_1 is G-conjugate to nh_2 if and only if h_1 and h_2 are $\mathbf{N}_H(C)$-conjugate.

2. *If $\{C_i \mid 1 \leq i \leq k\}$ is a complete set of representatives of the action of G on $\mathrm{Cl}(N)$, and $\{h_{ij} \mid 1 \leq j \leq k_i\}$ is a complete set of representatives of conjugacy classes of $H_i = \mathbf{N}_H(C_i)$, then $n_i h_{ij}$ is a complete set of representatives of the conjugacy classes of G, where $C_i = \mathrm{Cl}_N(n_i)$ and $[n_i, H_i] = 1$.*

Proof. Observe that N has a complement H in G by Schur-Zassenhaus theorem. First we show part 1. Observe that $\mathbf{N}_G(C) = N\mathbf{N}_H(C)$ and $\mathbf{N}_H(C)$ acts coprimely on N. By the comments before the lemma, since C is a conjugacy class of N which is $\mathbf{N}_H(C)$-invariant, there exist $n \in C$ which is fixed by $\mathbf{N}_H(C)$. Suppose that $nh_2 = (nh_1)^g$, for some $g \in G$. Since $(o(n), o(h_i)) = 1$ and n commutes with $h_i \in \mathbf{N}_H(C)$, where $i = 1, 2$, we have that $n^g = n$ and $h_1^g = h_2$. If $g = mh$ for $m \in N$ and $h \in H$, then

$$(h_1)^m = (h_2)^{h^{-1}} \in H \cap H^m = \mathbf{C}_H(m).$$

Hence $h_1^h = h_2$. Now, $(n^m)^h = n$ implies that $h \in \mathbf{N}_H(C)$. Since $[n, \mathbf{N}_H(C)] = 1$, the converse follows easily.

Now we prove part 2. Suppose that $x \in G$, and we prove that x is G-conjugate to some $n_i h_{ij}$, following the notation in the statement. We have that $x = nu$ for some $n \in N$ and $[u, n] = 1$, where $(o(u), o(n)) = 1$. By conjugating by an appropriate element, we may assume that $n = n_i$ for some i. Now, $H_i \subseteq \mathbf{C}_G(n_i)$ and $u \in \mathbf{C}_G(n_i)$. Since H_i is a π-complement of $\mathbf{C}_G(n_i) \subseteq \mathbf{N}_G(C_i)$ and u is a π'-element (where π is the set of primes dividing $|N|$), it follows by Schur-Zassenhaus theorem that $u^v \in H_i$ for some $v \in \mathbf{C}_G(n_i)$. Now $u^{vw} = h_{ij}$ for some $w \in H_i$. Now,

$$x^{vw} = n_i^{vw} h_{ij} = n_i h_{ij}.$$

Finally, if $n_i h_{ij}$ is G-conjugate to $n_r h_{rs}$, it is clear that $n_i = n_r$, and the result now follows from part 1. ∎

Now we are able to describe the rational classes of a group having a normal π-complement, for π a set of primes. We need the following technical result.

Lemma 2.9. *Suppose that $N \lhd G$ with $(|G:N|, |N|) = 1$ and let H be a complement of N in G. Let C be a conjugacy class of N, and write $C = \mathrm{Cl}_N(n)$ where $[n, \mathbf{N}_H(C)] = 1$. Let $h \in \mathbf{N}_H(C)$. Let also $g \in \mathbf{N}_G(C)^*$ with $g = ym$, where $m \in N$ and*

$$y \in \mathbf{N}_H(C)^* = \mathbf{N}_G(C)^* \cap H\,.$$

If $n^g \in \mathbf{C}_N(h)$, then there exists $z \in \mathbf{C}_N(h)$ such that $n^g = n^{yz}$.

Proof. Since $\mathbf{N}_H(C) \lhd \mathbf{N}_H(C)^*$, it is clear that $h^{y^{-1}} \in \mathbf{N}_H(C)$. Then $[n, h^{y^{-1}}] = 1$, or equivalently $[n^y, h] = 1$. Thus $n^y \in \mathbf{C}_N(h)$, and since n^g and n^y are N-conjugate, we deduce by Corollary 13.10 of [14] that n^g and n^y are indeed $\mathbf{C}_N(h)$-conjugate. Thus there exists $z \in \mathbf{C}_N(h)$ such that $n^{yz} = n^g$, as desired. ∎

Theorem 2.10. *Suppose that $N \lhd G$ with $(|G:N|, |N|) = 1$ and let H be a complement of N in G. Let C be a conjugacy class of N, and write $C = \mathrm{Cl}_N(n)$ where $[n, \mathbf{N}_H(C)] = 1$. Suppose that C^G is rational. If $h \in \mathbf{N}_H(C)$, then $\mathrm{Cl}_G(nh)$ is rational if and only if $L = \mathrm{Cl}_{\mathbf{N}_H(C)}(h)$ is rational and invariant in $\mathbf{N}_H(C)^* = \mathbf{N}_G(C)^* \cap H$.*

Proof. Suppose first that $\mathrm{Cl}_G(nh)$ is rational. Suppose that $\langle h^k \rangle = \langle h \rangle$, and we want to see that h^k is $\mathbf{N}_H(C)$-conjugate to h. By using the Chinese Remainder theorem, we may assume that $n^k = n$. Now, since nh is rational in G, we have that $(nh)^k = nh^k$ is G-conjugate to nh, and we deduce from Lemma 2.8 that h and h^k are $\mathbf{N}_H(C)$-conjugate, as desired.

Next we prove that L is $\mathbf{N}_H(C)^*$-invariant. Let $y \in \mathbf{N}_H(C)^*$. Then $\mathrm{Cl}_N(n^y) = \mathrm{Cl}_N(n^t)$ for some integer t coprime to $o(n)$. Again using the Chinese Remainder theorem, we may assume that $h^t = h$. So $n^t = n^{ym}$ for some $m \in N$, and we can suppose by Lemma 2.9 that $m \in \mathbf{C}_N(h)$. Now nh is rational in G, and therefore G-conjugate to

$$(nh)^t = n^t h = n^{ym} h = (nh^{y^{-1}})^{ym}.$$

We deduce that $\mathrm{Cl}_G(nh) = \mathrm{Cl}_G(nh^{y^{-1}})$. Now it follows from Lemma 2.8 that h is $\mathbf{N}_H(C)$-conjugate to $h^{y^{-1}}$. This implies that L is y-invariant, as desired.

Conversely, suppose now that L is rational and $\mathbf{N}_H(C)^*$-invariant. We want to prove that $\mathrm{Cl}_G(nh)$ is rational. Suppose that $\langle nh \rangle = \langle (nh)^k \rangle$. Note that $\langle h^k \rangle = \langle h \rangle$, and then $h^k = h^v$ for some $v \in \mathbf{N}_H(C)$, since L is rational. Thus we have $(nh)^k = n^k h^v$. Also, since n is rational in G, we know that there exists $g \in \mathbf{N}_G(C)^*$ such that $n^k = n^g$. Write $g = ym$, where $y \in \mathbf{N}_H(C)^*$ and $m \in N$. Since $n^g = n^k \in \mathbf{C}_N(h^v)$, we can assume by Lemma 2.9 that $m \in \mathbf{C}_N(h^v)$. Now

$$(nh)^k = n^g h^v = (nh^{vy^{-1}})^g,$$

and we deduce that $(nh)^k$ is G-conjugate to $nh^{vy^{-1}}$. Since L is $\mathbf{N}_H(C)^*$-invariant, it follows that $h^{vy^{-1}}$ is $\mathbf{N}_H(C)$-conjugate to h. This implies by Lemma 2.8 that $nh^{vy^{-1}}$ is G-conjugate to nh, and we deduce that $(nh)^k$ and nh are G-conjugate, as desired. ▮

With the same notation as in Theorem 2.10, if $n \in N$ and $C = \mathrm{Cl}_N(n)$, then the number of rational conjugacy classes of G which have π-part n is exactly the number of rational classes of $\mathbf{N}_H(C)$ which are invariant under the action of $\mathbf{N}_H(C)^*$. In particular, this number equals $|\mathrm{Cl}_{\mathbf{Q}}(\mathbf{N}_H(C))|$ if $\mathbf{N}_H(C)^*$ is abelian. This observation should be compared with the statement of Corollary 2.6.

2.3 Main Results

We now work towards a proof of Theorem A. The following key result has a proof inspired on an idea by T. Wilde in [37], where he studied the real part of a character table.

Theorem 2.11. *Suppose that P is a group that acts coprimely as automorphisms on N, and let $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|N|}/\mathbb{Q})$. Then the actions of $P \times \langle\sigma\rangle$ on $\mathrm{Irr}(N)$ and $\mathrm{Cl}(N)$ are permutation isomorphic.*

Actually, we shall need a more general version of Theorem 2.11, where only certain characters and classes of N are taken into account. In order to obtain that version, we need to use Isaacs B_π-characters (see Section 1.5). In fact, we shall need the existence of an extension of the Glauberman-Isaacs correspondence in the frame of π-theory (see Theorem 1.14).

Theorem 2.12. *Suppose that a group A acts on a π-separable group G and $(|A|, |G|) = 1$. Then there exists a canonical bijection between the A-invariant B_π-characters of G and the B_π-characters of $\mathbf{C}_G(A)$, the subgroup of fixed points of A in G.*

The word "canonical" in Theorem 2.12 means that any choice made in the construction of the correspondence leads to the same bijection; in particular, the correspondence commutes with automorphism action and with Galois action, as it can be easily checked. Theorem 2.12 was proved by T. Wolf in [38], and later generalized in [10].

Note that we can recover Theorem 2.11 by taking π to be the set of all primes dividing $|N|$ in the next result. We denote by $\mathrm{Cl}_\pi(N)$ the set of conjugacy classes of N consisting of π-elements.

Theorem 2.13. *Suppose that a group Q acts coprimely as automorphisms on a π-separable group N, and let $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|N|}/\mathbb{Q})$. Then the natural actions of $Q \times \langle\sigma\rangle$ on $B_\pi(N)$ and on $\mathrm{Cl}_\pi(N)$ are permutation isomorphic.*

Proof. It is enough to show that if H is a subgroup of $Q \times \langle\sigma\rangle$, then H fixes the same number of characters in $B_\pi(N)$ as of classes in $\mathrm{Cl}_\pi(N)$, by Lemma 1.13. Let $\pi : H \to \langle\sigma\rangle$ be the restriction to H of the projection of $Q \times \langle\sigma\rangle$ onto $\langle\sigma\rangle$, and write X for the kernel of π. Since H/X is a cyclic group, there exists $\rho = (z, \sigma^k) \in H$ such that $H = X\langle\rho\rangle$, where $z \in Q$ and k is an integer.

Observe that X acts coprimely on N, and thus Theorem 2.12 applies. The Glauberman-Isaacs bijection, from the B_π-characters of N which are X-invariant onto the B_π-characters

$\mathbf{C}_N(X)$, commutes with Galois action and with action induced by automorphisms of N on characters and classes, so in particular it commutes with the action of $\langle\rho\rangle$. It then follows that the number of H-fixed B_π-characters of N equals the number of $\langle\rho\rangle$-fixed B_π-characters of $\mathbf{C}_N(X)$. Similarly, the map $C \mapsto C \cap \mathbf{C}_N(X)$ is a bijection form the set of X-invariant conjugacy classes of π-elements N onto the set of conjugacy classes of π-elements of $\mathbf{C}_N(X)$, and this map also commutes with the action of $\langle\rho\rangle$. In particular, the number of H-invariant conjugacy classes of N containing π-elements equals the number of $\langle\rho\rangle$-fixed classes of π-elements of $\mathbf{C}_N(X)$.

The result now follows from of Brauer's Permutation Lemma for B_π-characters and classes of π-elements, Theorem 1.18, applied to the action of $\langle\rho\rangle$ on $\mathbf{C}_N(X)$. ▌

Let us now make a useful remark that will be needed later on. Let g be an element of a group G, and suppose that g has order k. As usual, write $\mathcal{G}_k = \mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q})$, where $\mathbb{Q}_k$ is the kth cyclotomic extension of the rationals. By the discussion at the beginning of Section 1.4, the map

$$\begin{array}{ccc} \mathcal{G}_k & \longrightarrow & \mathrm{Aut}(\langle g\rangle) \\ \sigma & \mapsto & f \end{array} \tag{2.3}$$

defined by $f(g) = g^t$ when $\xi^\sigma = \xi^t$, where ξ is a primitive complex kth root of unity and $1 \le t \le k$ is an integer coprime to k, is a well-defined group isomorphism. As usual, we write $\sigma = \sigma_t$ if $\xi^\sigma = \xi^t$. It is clear that the map

$$\begin{array}{ccc} \mathbf{N}_G(\langle g\rangle) & \longrightarrow & \mathrm{Aut}(\langle g\rangle) \\ y & \mapsto & f \end{array} \tag{2.4}$$

given by $f(g) = g^y$ defines a group homomorphism with kernel $\mathbf{C}_G(g)$, so we can identify $\mathbf{N}_G(\langle g\rangle)/\mathbf{C}_G(g)$ with a subgroup of $\mathrm{Aut}(\langle g\rangle)$.

Arguing as in in the beginning of Section 2.2.2, one can check that $\mathcal{G}_k$ acts naturally on the set of conjugacy classes of G containing elements whose order is a divisor of k, via

$$\mathrm{Cl}_G(x)^{\sigma_t} = \mathrm{Cl}_G(x^t)\,,$$

with the same notation as before. Let C be the conjugacy class of g in G, and note that $\mathbb{Q}(C)$ is contained in $\mathbb{Q}_k$, by 1.5. The stabilizer of C is $\mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q}(C))$, arguing as in Section 2.2.2. We claim that the restriction of the isomorphism 2.3

$$\mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q}(C)) \longrightarrow \mathrm{Aut}(\langle g\rangle) \tag{2.5}$$

has image $\mathbf{N}_G(\langle g\rangle)/\mathbf{C}_G(g)$. In fact, if $\sigma_t \in \mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q}(C))$ then

$$\mathrm{Cl}_G(g) = \mathrm{Cl}_G(g)^{\sigma_t} = \mathrm{Cl}_G(g^t)\,,$$

and thus $g^t = g^y$ for some $y \in \mathbf{N}_G(g)$. So it is clear that the image of 2.5 is contained in $\mathbf{N}_G(\langle g\rangle)/\mathbf{C}_G(g)$, by definition of 2.4. Conversely, let $y\mathbf{C}_G(g) \in \mathbf{N}_G(\langle g\rangle)/\mathbf{C}_G(g)$, so $g^y = g^s$ for a unique $1 \le s \le k$ coprime to k, by 2.4. Now, if $\sigma \in \mathcal{G}_k$ with $\sigma = \sigma_s$, we have that

$$C^\sigma = \mathrm{Cl}_G(g^s) = \mathrm{Cl}_G(g^y) = C\,,$$

so we deduce that $\sigma \in \mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q}(C))$, as wanted. We have just proved that the map

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q}(C)) & \longrightarrow & \mathbf{N}_G(\langle g\rangle)/\mathbf{C}_G(g) \\ \sigma & \mapsto & y\mathbf{C}_G(g) \end{array} \tag{2.6}$$

defined by $g^y = g^t$ when $\xi^\sigma = \xi^t$, with the above notation, is a group isomorphism.

We can now continue to work toward the proof of the main results in this chapter. The following crucial observation appears in [28], and explains why we need to introduce B_π-characters. The next result is contained in Lemma 2.1 and Theorem 2.2 of [28].

Theorem 2.14. *Suppose that G has a cyclic Sylow 2-subgroup, and let N be the normal 2-complement of G. Let $1 \neq \theta \in \mathrm{Irr}(N)$, $n \in N$ and $C = \mathrm{Cl}_N(n)$.*

1. *If C^G is rational, then n is a p-element for some prime p.*
2. *If θ^G is rational valued, then $\theta \in B_p(N)$ for a unique p.*

Proof. First we prove part 1 in the statement. With the above notation, if C^G is rational and $\mathcal{H} = \mathrm{Gal}(\mathbb{Q}(C)/\mathbb{Q})$, then by Lemma 2.7 we have that

$$\mathcal{H} \cong \mathbf{N}_G(C)^*/\mathbf{N}_G(C)\,.$$

Observe that $N \leq \mathbf{N}_G(C)$, so $\mathbf{N}_G(C)^*/\mathbf{N}_G(C)$ is a cyclic 2-group, because G has cyclic Sylow 2-subgroups. Write $k = o(n)$, which is an odd integer. Also, let $\mathcal{G} = \mathcal{G}_k = \mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q})$, and note that $\mathcal{G}$ is abelian. Let $\mathcal{K}$ be the normal 2-complement of $\mathcal{G}$. For any $\sigma \in \mathcal{H}$, there exists an integer t coprime to k such that $\xi^\sigma = \xi^t$, where $\xi \in \mathbb{C}$ has order k, and as usual we write $\sigma = \sigma_t$. By 2.6, the map

$$\mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q}(C)) \longrightarrow \mathbf{N}_N(\langle n\rangle)/\mathbf{C}_N(n)$$

given by $\sigma_t \mapsto g\mathbf{C}_N(n)$ when $n^t = n^g$, is a well-defined group isomorphism. In particular we have that

$$|\mathbf{N}_N(\langle n\rangle)/\mathbf{C}_N(n)| = |\mathbb{Q}_k : \mathbb{Q}(C)|\,,$$

and therefore the degree on the right side of the equality is odd. Hence

$$\mathcal{U} = \mathrm{Gal}(\mathbb{Q}_k/\mathbb{Q}(C)) \leq \mathcal{K}\,.$$

By elementary Galois theory $\mathcal{G}/\mathcal{U} \cong \mathcal{H}$, which is cyclic. Then since $\mathcal{U} \leq \mathcal{K}$, we conclude that $\mathcal{G}$ has a cyclic Sylow 2-subgroup. Finally, if $k = p_1^{e_1}\cdots p_s^{e_s}$ is the decomposition of k as product of different (odd) primes, then $\mathcal{G} \cong \mathcal{G}_{p_1^{e_1}} \times \cdots \times \mathcal{G}_{p_s^{e_s}}$ has a cyclic Sylow 2-subgroup if and only if k is a prime power, and part 1 follows.

Now we show part 2. Write $\mathcal{J} = \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$. If θ^G is rational, then $T^*/T \cong \mathcal{J}$ is cyclic. By elementary character theory, we have that complex conjugation is an automorphism of $\mathbb{Q}(\theta)$. Since N has odd order and $1 \neq \theta$, we have that this automorphism σ is non-trivial. Hence, σ is the only involution of $\mathcal{J}$.

Now let $K = \ker(\theta) < N$. Let M/K be a minimal normal subgroup of N/K. Hence M/K is an elementary abelian p-group for some prime p. We claim that $\theta \in B_p(N)$. Let $1 \neq \lambda \in \mathrm{Irr}(M)$ be linear under θ. It is enough to show that $\theta^\tau = \theta$, where $\tau \in \mathcal{J}$ fixes

p-power roots of unity and complex conjugates p'-roots of unity, by Theorem 1.22. Since $\mathcal{J}$ has a unique involution, we conclude that $\tau \in \langle\sigma\rangle$. Thus $\theta^\tau = \theta$ or $\theta^\tau = \bar{\theta}$. Suppose that $\theta^\tau = \bar{\theta}$. Then $\overline{\theta^\tau} = \theta$, and we deduce that $\overline{\lambda^\tau}$ and λ are irreducible constituents of θ_M. By Clifford's Theorem 1.7, and using that $\lambda^\tau = \lambda$, we have that $\bar{\lambda} = \lambda^n$ for some $n \in N$. Hence $\lambda^{n^2} = \lambda$, and since N has odd order we have that $\lambda^n = \lambda = \bar{\lambda}$, and $\lambda = 1$. This is a contradiction. Now, if $\theta \in B_q(N)$ for some other prime q, then $\mathbf{O}_p(N/K)$ would be contained in the kernel of θ, and this is impossible. ▮

Lemma 2.15. *Suppose that N is a normal Hall subgroup of G. Suppose that p is an odd prime and let σ be a generator of the cyclic Galois group* $\mathrm{Gal}(\mathbb{Q}_{p^a}/\mathbb{Q})$.

1. *If $\theta \in \mathrm{Irr}(N)$ has values in $\mathbb{Q}_{p^a}$, then θ^G is rational if and only if $\theta^\sigma = \theta^y$ for some $y \in G$.*
2. *If $n \in N$ is a p-element of order dividing p^a, then $\mathrm{Cl}_G(n)$ is rational if and only if $\mathrm{Cl}_N(n)^\sigma = \mathrm{Cl}_N(n)^y$ for some $y \in G$.*

Proof. We know that the equation $\theta^g = \theta^\tau$ defines a map

$$T^* \longrightarrow \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G))\,.$$

In case 1, $\tau = \sigma_{\mathbb{Q}(\theta)} \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G))$. Since τ generates $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$, part 1 follows. Part 2 is proved similarly using Lemma 2.7. ▮

Now we are able to prove Theorem A.

Theorem 2.16. *Suppose that G has a cyclic Sylow 2-subgroup Q. Then* $|\mathrm{Irr}_{\mathbb{Q}}(G)| = |\mathrm{Cl}_{\mathbb{Q}}(G)|$.

Proof. Let N be the normal 2-complement of G. If p is an odd prime, let $\mathrm{Irr}_{\mathbb{Q},p}(G)$ be the set of rational valued $\chi \in \mathrm{Irr}(G)$ lying over some non-trivial B_p-character $\theta \in B_p(N)$. By Lemma 2.4 and Theorem 2.14, we have that $\mathrm{Irr}_{\mathbb{Q}}(G)$ is the disjoint union

$$\mathrm{Irr}_{\mathbb{Q}}(G) = \mathrm{Irr}_{\mathbb{Q}}(G/N) \cup \bigcup_{p\,||N|} \mathrm{Irr}_{\mathbb{Q},p}(G)\,.$$

Notice that $\mathrm{Irr}_{\mathbb{Q}}(G/N)$ has size 2. Also, let $\mathrm{Cl}_{\mathbb{Q},p}(G)$ the set of rational classes $\mathrm{Cl}_G(x)$ such that $1 \neq x_{2'}$ is a p-element of N. Suppose that $\mathrm{Cl}_G(x)$ is rational, and write $x = nh$, where $[n,h] = 1$ and $h \in Q$. Since $n = x_{2'}$ is rational (because it is a power of a rational element) we have that n is a p-element by Theorem 2.14. Now, observe that $n = 1$ if and only if x is a rational 2-element, if and only if $\mathrm{Cl}_G(x)$ is either the class of 1_G or the unique class of involutions of G, because a 2-element of G of order bigger than 2 is not conjugate to its inverse in G. Hence

$$|\mathrm{Cl}_{\mathbb{Q}}(G)| = 2 + \sum_{p\,||N|} |\mathrm{Cl}_{\mathbb{Q},p}(G)|\,.$$

It suffices then to show that

$$|\mathrm{Irr}_{\mathbb{Q},p}(G)| = |\mathrm{Cl}_{\mathbb{Q},p}(G)|\,.$$

Let $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{Q}_{|G|_p}/\mathbb{Q})$. By Theorem 2.13, we have that the actions of $Q \times \langle\sigma\rangle$ on $B_p(N)$ and $\mathrm{Cl}_p(N)$ are permutation isomorphic. Hence, using Lemma 2.15, we may choose representatives $\{\theta_i\}_{1\le i\le s}$ of the Q-action on the $B_p(N)$-characters lying under rational characters of G, and representatives $\{C_i\}_{1\le i\le s}$ of the conjugacy classes of p-elements of N with C_i^G being rational, such that $\mathbf{N}_G(C_i) = I_G(\theta_i)$ and $\mathbf{N}_G(C_i)^* = I_G(\theta_i)^*$. We have that

$$|\mathrm{Irr}_{\mathbf{Q},p}(G)| = \sum_{i=1}^{s} |\mathrm{Irr}_{\mathbf{Q}}(G|\theta_i)|$$

and

$$|\mathrm{Cl}_{\mathbf{Q},p}(G)| = \sum_{i=1}^{s} |\{\mathrm{Cl}_G(x) \,|\, x \text{ is rational and } x_p \in C_i\}|\,.$$

Now Corollary 2.6 and Theorem 2.10 imply that each of the summands in the above sums equals 2, because $\mathbf{N}_G(C_i)^* \cap Q$ is a cyclic 2-group, and the result follows. ∎

2.4 Some remarks and an example

As mentioned in Section 2.1, working in a similar fashion as before it is possible to prove the following result.

Theorem 2.17. *Suppose that G has a normal Sylow p-subgroup P, where p is odd. Suppose that for every section $X \lhd Y \subseteq G/P$, where Y/X is abelian, the number of Y-invariant rational characters of X is the number of Y-invariant rational classes of X. Then $|\mathrm{Irr}_{\mathbf{Q}}(G)| = |\mathrm{Cl}_{\mathbf{Q}}(G)|$.*

Sketch of proof. Let H be a complement of P in G. By Theorem 2.10, the number of $\mathrm{Cl}_G(x) \in \mathrm{Cl}_{\mathbf{Q}}(G)$ with $x_p = 1$ is $|\mathrm{Cl}_{\mathbf{Q}}(H)|$, and by hypothesis this equals $|\mathrm{Irr}_{\mathbf{Q}}(G/P)|$. Then we need to show that the two sets

$$\{\chi \in \mathrm{Irr}_{\mathbf{Q}}(G) \,|\, P \not\leq \ker(\chi)\},\ \{\mathrm{Cl}_G(x) \in \mathrm{Cl}_{\mathbf{Q}}(G) \,|\, x_p \neq 1\}$$

have the same size.

Let $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{Q}_{|P|}/\mathbb{Q})$, and recall that by Theorem 2.11 $\langle\sigma\rangle \times H$ acts permutation isomorphically on the two sets $\mathrm{Cl}(P)$ and $\mathrm{Irr}(P)$. Hence, using Lemma 2.15, we may choose representatives $\{\theta_i\}_{1\le i\le s}$ of the H-action on the irreducible characters of P lying under rational characters of G, and $\{C_i\}_{1\le i\le s}$ representatives of the H-action on the conjugacy classes of P with C_i^G being rational, such that $\mathbf{N}_G(C_i) = I_G(\theta_i) = T_i$ and $\mathbf{N}_G(C_i)^* = T_i^*$, where T_i^* is the semi-inertia group of θ in G. Of course T_i^*/T_i is abelian, and so by hypothesis the number of T_i^*-invariant rational characters of T_i equals the number of T_i^*-invariant classes of T_i. The result now follows from Corollary 2.6 and Theorem 2.10. ∎

For instance, if G/P is an abelian group then for every section $X \lhd Y \subseteq G/P$ the number of rational conjugacy classes of X equals the number of rational irreducible characters of X, and all of them are Y-invariant.

Suppose that X is a group such that there is a bijection

$$f : \mathrm{Irr}_{\mathbb{Q}}(X) \longrightarrow \mathrm{Cl}_{\mathbb{Q}}(X) \tag{2.7}$$

satisfying $f(\chi^a) = C^a$ for any $\chi \in \mathrm{Irr}_{\mathbb{Q}}(X)$ and $a \in \mathrm{Aut}(X)$, whenever $f(\chi) = C \in \mathrm{Cl}_{\mathbb{Q}}(X)$. Then any subgroup $H \leq \mathrm{Aut}(X)$ fixes the same number of characters in $\mathrm{Irr}_{\mathbb{Q}}(G)$ than classes in $\mathrm{Cl}_{\mathbb{Q}}(X)$. In particular, if $X \lhd Y$ it follows that the number of Y-invariant rational characters of X is the number of Y-invariant rational classes of X.

Lemma 2.18. *Suppose that X is either a dihedral, semi-dihedral or generalized quaternion 2-group. Then there exists a bijection*

$$f : \mathrm{Irr}_{\mathbb{Q}}(X) \longrightarrow \mathrm{Cl}_{\mathbb{Q}}(X)$$

as in 2.7.

Proof. Suppose first that X is the quaternion group of order 8. Then every element of X is rational, and X has a unique involution and three classes containing elements of order 4. Also, X has three non-principal linear characters and an irreducible character of degree two. Observe that each non-principal linear character contains a unique class of elements of order 4 inside the kernel, and that these classes are distinct for distinct characters, so it is obvious how to construct the natural map.

Suppose now that X is not the quaternion group of order 8. Let H be the unique cyclic maximal subgroup of X. The rational classes of X contained in H are $\mathrm{Cl}_X(1)$, $\mathrm{Cl}_X(z)$ and $\mathrm{Cl}_X(x)$, where $o(z) = 2$ and $o(x) = 4$. There are two more rational classes in X, namely $C_1 = \mathrm{Cl}_X(a_1)$ and $C_2 = \mathrm{Cl}_X(a_2)$, where C_1 and C_2 are the only conjugacy classes of X lying outside H.

Let $\lambda \in \mathrm{Irr}(H)$ be the unique character of H with $o(\lambda) = 2$, and write $\chi_1, \chi_2 \in \mathrm{Irr}(X)$ for the unique characters of X lying over λ, which actually extend λ. Write also $\psi \in \mathrm{Irr}(X)$ for the unique character of X lying over some $\varphi \in \mathrm{Irr}(H)$ with $o(\varphi) = 4$, and let $1_G \neq \delta \in \mathrm{Irr}(G/H)$. Then it is easy to check that $1_G, \delta, \psi, \chi_1$ and χ_2 are all the rational characters of X.

Observe that $\mathrm{Cl}_X(1)$, $\mathrm{Cl}_X(z)$, $\mathrm{Cl}_X(x)$ and $1_G, \delta, \psi$ are invariant under automorphism action. Also, we can assume that $a_i \in \ker(\chi_i)$ and $a_i \notin \ker(\chi_j)$ for $i, j = 1, 2$, as it is easy to check. Then any bijection

$$f : \mathrm{Irr}_{\mathbb{Q}}(X) \longrightarrow \mathrm{Cl}_{\mathbb{Q}}(X)$$

with $f(\chi_i) = C_i$ for $i = 1, 2$ is as wanted. ∎

We shall need to use the following observation, which is routine to prove.

Lemma 2.19. *Let G be either a dihedral, semi-dihedral or generalized quaternion 2-group. Then any subgroup $X \leq G$ is either cyclic, dihedral, semi-dihedral, generalized quaternion or isomorphic to $C_2 \times C_2$.*

Of course, if X is a cyclic 2-group then there is a natural bijection between the rational classes of X and the irreducible rational characters of X. Also, it is not difficult to construct a natural correspondence between the rational classes and the rational irreducible characters of $C_2 \times C_2$, by looking at the kernels of the rational characters. We therefore have the following:

Theorem 2.20. *Suppose that $G = PQ$, where $P \lhd G$ is a Sylow p-subgroup of G, for p an odd prime, and Q is either an abelian, dihedral, semi-dihedral or generalized quaternion 2-group. Then $|\mathrm{Irr}_{\mathbf{Q}}(G)| = |\mathrm{Cl}_{\mathbf{Q}}(G)|$.*

Proof. This follows from Theorem 2.17, Lemma 2.18, Lemma 2.19 and the comments above. ∎

We close this chapter with an example which shows that we cannot extend much our hypotheses in Theorem A.

Example 2.21. *There is a finite group G of order $2^2 \cdot 3^4 \cdot 7$ with an elementary abelian Sylow 2-subgroup, having a normal 2-complement and such that the number of rational characters of G is not the number of rational classes of G.*

Let $X = \langle u, v, w \rangle = C_9 \times C_3 \times C_7$, where $o(u) = 9$, $o(v) = 3$ and $o(w) = 7$. Consider the automorphism σ of X of order 3 with $u^\sigma = u$, $v^\sigma = u^3 v$, $w^\sigma = w^2$. Now consider the automorphisms τ, ρ of order 2 such that τ inverts the 3-elements of X and fixes the 7-elements, and ρ fixes the 3-elements but inverts the 7-elements. Then it can be checked in GAP [8] that the semidirect product

$$G = X\langle \sigma, \tau, \rho \rangle$$

has 15 rational classes and 18 rational characters. Now, since $Q_8/\mathbf{Z}(Q_8) = C_2 \times C_2 = D_8/\mathbf{Z}(S_8)$, we can modify this group to obtain similar examples with dihedral or quaternion Sylow 2-subgroups.

Chapter 3

2-Length and rational characters of odd degree

3.1 Introduction

It is a well-known fact that a group G has odd order precisely when the principal character is the unique rational irreducible character of G. The fact that the proof of this result requires the Classification of the Finite Simple Groups (see [31], for instance), illustrates the difficulties that rationality questions may involve. A refinement of this result was suggested in a rather old conjecture by R. Gow, who predicted that every finite group of even order has a non-trivial rational irreducible character of odd degree.

Recently, R. Gow's conjecture was shown to be true by G. Navarro and P. H. Tiep in [31]. In order to prove the conjecture, the authors introduced new techniques to extend rational characters, which permitted to prove a stronger version of the result for solvable groups. More precisely, G. Navarro and P. H. Tiep showed that if G is a solvable group of even order, then the 2-length of G is less than the number of rational irreducible characters of G of odd degree.

Our main purpose in this chapter is to present a significant improvement of the result by G. Navarro and P. H. Tiep. We shall show that there exists a logarithmic upper bound for the 2-length of a solvable group G, in terms of the number of rational characters of G of odd degree.

Theorem B. *Let G be a solvable group, and assume that the 2-length of G is $l \in \mathbb{N}$. Then G has at least 2^l rational characters of odd degree.*

This result has some interesting consequences, treated in Section 3.4 below. For instance, Theorem B gives a perhaps unexpected new global/local relationship, not involving characters in its statement: if P is a Sylow 2-subgroup of a solvable group G, then the number of orbits in $P/\Phi(P)$ under the action of the normalizer of P in G admits a logarithmic bound by the 2-length of G.

It is an immediate corollary of a theorem of J. Thompson (IX.8.6 of [12]) that a solvable group with only two rational conjugacy classes has 2-length one. Recent work by M. Isaacs and G. Navarro [18] shows that the same conclusion holds for a solvable

group with at most three conjugacy classes of rational elements. As the authors of [18] demonstrate, this can be proved using our Theorem B.

Once Theorem B is established, it seems natural to ask if the bound that the result provides is accurate. As we shall see in Section 3.5, there exist examples showing that this bound is best possible. We shall also discuss some generalizations of the above results to arbitrary primes in Section 3.3.

The main results in this chapter, including Theorem B above, have been published in [34]. The generalization of Theorem B to arbitrary primes appears in [33].

3.2 Main Result

Suppose that G is a finite group and let $\chi \in \mathrm{Irr}(G)$ be non-principal and real-valued. Then a theorem of Burnside guarantees that G has even order, and indeed this is not difficult to prove. Working by contradiction, suppose that $|G|$ is odd. Note that by the orthogonality relations we have that

$$0 = |G|\,[1_G, \chi] = \chi(1) + \sum_{g \in G \setminus \{1\}} \chi(g)\,.$$

Since χ is real-valued, we have that $\chi(g) = \chi(g^{-1})$ for every $g \in G$. It follows from the assumption that G has odd order that G does not contain any involution, and thus the second summand above equals 2α, for some algebraic integer α (either by basic character theory or by Brauer's Theorem 10.3 of [13]). So α is a rational integer and $\chi(1)$ is even. In particular $|G|$ is even by Theorem 1.4, which gives the desired contradiction.

We note that the converse of Burnside's theorem admits an elementary proof based on Brauer's permutation lemma on character tables, Theorem 1.12. In fact, observe that if G has even order, then G contains an involution, and of course an involution is a real element. Then, Brauer's lemma implies that G has a non-trivial real-valued irreducible character.

We also observe that Brauer's Theorem 1.12 on character tables provides an alternative proof of Burnside's result. It is immediate that the centralizer of a non-trivial odd-order real element of G has even index in the normalizer of that element in G, and hence G has even order if G contains a non-trivial real element. By Brauer's Theorem 1.12, if G has a non-principal real-valued irreducible character, then G has a non-trivial real element, and thus $|G|$ is even.

Generally speaking, rationality questions in finite groups are somehow more delicate than those concerning real values, although our problem essentially deals with real-valued characters. As it was pointed out in the previous section, some results aimed to producing rational characters can be found in Section 2 of [31]. Next we include some of the techniques on extension of rational characters required to prove Theorem B, and we refer the reader to [31] for further details.

The general setting is as follows. We start with a rational character of a normal subgroup N of G, and the goal is to find conditions to extend it to a rational character of the whole group; of course, we need to assume that our original character is invariant

in G. If $N \lhd G$ and $\psi \in \mathrm{Irr}(N)$, we recall that $\mathrm{Irr}(G|\psi)$ is the set of irreducible characters of G lying over ψ.

Lemma 3.1. *Let $N \lhd G$ with G/N of odd order. If $\psi \in \mathrm{Irr}(N)$ is rational valued, then there exists a unique rational character χ in $\mathrm{Irr}(G|\psi)$.*

Proof. See Corollary 2.2 of [30]. ∎

If we drop the assumption that the index of N in G is odd, then we need additional hypotheses to guarantee the existence of rational extensions. The cyclic group of order four is an illustrative example: the non-trivial character of the unique subgroup of index two of such group does not admit any rational extension to the whole group.

Lemma 3.2. *Let N be a normal subgroup of G, and let $\theta \in \mathrm{Irr}(N)$ be invariant in G. Suppose that θ is rational of odd degree, and assume also that $o(\theta) = 1$. Then there exists a rational extension $\chi \in \mathrm{Irr}(G)$ of θ.*

Proof. See Corollary 2.4 of [30]. ∎

Before starting to work towards the proof of Theorem B, let us recall the definition of the **p-length** of a solvable group, where p is any prime. For any group G, we write $\mathbf{O}^p(G)$ to denote the unique normal subgroup of G with index in G a power of p and minimal satisfying this condition. Similarly, let $\mathbf{O}^{p'}(G)$ be the unique normal subgroup of G with index in G not divisible by p and minimal with this condition. We write $\mathbf{O}^{pp'}(G) = \mathbf{O}^{p'}(\mathbf{O}^p(G))$. Note that $\mathbf{O}^{pp}(G) = \mathbf{O}^p(G)$, and an analogue equality holds for $\mathbf{O}^{p'}(G)$. As it is well-known, if G is solvable then the series

$$G \geq \mathbf{O}^{p'}(G) \geq \mathbf{O}^{p'p}(G) \geq \mathbf{O}^{p'pp'}(G) \geq \cdots$$

eventually reaches the trivial subgroup of G. In particular, for G solvable either $\mathbf{O}^p(G)$ or $\mathbf{O}^{p'}(G)$ is a proper subgroup of G.

If G is a solvable group, write $G_0 = G$, $G_t = \mathbf{O}^{p'p}(G_{t-1})$ and $M_t = \mathbf{O}^{p'}(G_{t-1})$, for each $1 \leq t \in \mathbb{N}$. The p-length of G is defined as the smallest natural number l such that $M_{l+1} = 1$. Notice that G has p-length zero if and only if G has order not divisible by p.

One can alternatively define the p-length of G "starting from the bottom", that is considering normal subgroups of order either a power of p or not divisible by p, and maximal with this condition. The standard notation for these normal subgroups of G is $\mathbf{O}_p(G)$ and $\mathbf{O}_{p'}(G)$, respectively. The invariant obtained in both approaches, the p-length of G, is obviously the same, although the two series of normal subgroups do not need to coincide.

It seems convenient now to introduce some notation. Suppose that G is a group, $N \lhd G$ and $\psi \in \mathrm{Irr}(N)$. We write $\mathrm{Irr}_{2',\mathbb{Q}}(G)$ for the set of irreducible rational characters of G which have odd degree, and the set $\mathrm{Irr}_{2',\mathbb{Q}}(G|\psi)$ consists of the characters in $\mathrm{Irr}_{2',\mathbb{Q}}(G)$ which lie over ψ. More generally, if p is any prime, then $\mathrm{Irr}_{p',\mathbb{Q}_p}(G)$ is the set of p'-degree irreducible characters of G having values in the pth cyclotomic field $\mathbb{Q}_p$.

We shall use that if G is a p-group, then $\mathrm{Irr}_{p',\mathbb{Q}_p}(G) = \mathrm{Irr}(G/\Phi(G))$, where $\Phi(G)$ is the Frattini subgroup of G; this immediately follows from Theorem 1.4. In particular, every non-trivial 2-group has a non-principal rational character of odd degree.

Suppose that χ is a character of G afforded by a representation $\mathcal{X}$ of G. It is easy to see that

$$\mathcal{Y}(g) = \mathcal{X}(g^{-1})^t$$

defines a representation of G, where $g \in G$ and the superscript ^{t} denotes the transposed matrix. Also, $\mathcal{Y}$ affords the character $\overline{\chi}$. Assume now that that χ is real-valued, so $\mathcal{X}$ and $\mathcal{Y}$ are similar, by Theorem 1.3. Then

$$1 = \det(\mathcal{X}(g)\mathcal{X}(g^{-1})) = \det(\mathcal{X}(g))\det(\mathcal{Y}(g)) = \det(\mathcal{X}(g))^2,$$

for all $g \in G$, since both the transposed matrix M^t of a matrix M, and a matrix similar to M, have determinant $\det(M)$. It follows that $o(\chi)$ divies 2 if χ is real-valued.

Next we restate Gow's conjecture for solvable groups, which appeared in [31] as Theorem 3.1, and then give a proof of Theorem B. In order to prove Theorem B, we shall need to use the properties of canonical extensions discussed in Chapter 2 (see the comments before Corollary 2.6).

Lemma 3.3. *Let G be a solvable group of even order. Then G has at least two rational irreducible characters of odd degree.*

Proof. This follows from Theorem B below. See also Lemma 3.1 of [30]. ∎

Theorem B. *Let G be a solvable group, and assume that the 2-length of G is $l \in \mathbb{N}$. Then G has at least 2^l rational irreducible characters of odd degree.*

Proof. If $l = 0$ the result is trivial, so we can assume that G has even order.

We shall use the same notation as in the definition of the 2-length of G for the characteristic subgroups M_t, G_t of G.

Let P be a Sylow 2-subgroup, and notice that P acts by conjugation on the set of rational, linear characters of the non-trivial 2-group M_t/G_t, for every $1 \leq t \leq l$. This set of characters has even size, and it is clear that the trivial character 1_{M_t} is invariant under the action of P. Hence, it follows that P fixes a non-trivial linear character $\lambda_t \in \mathrm{Irr}(M_t/G_t)$ which is rational valued, for each $1 \leq t \leq l$.

We claim that if $\psi \in \mathrm{Irr}_{2',\mathbb{Q}}(M_t)$ is P-invariant, then the set $\mathrm{Irr}_{2',\mathbb{Q}}(G|\psi)$ has size at least 2^{t-1}, for $1 \leq t \leq l$. We proceed by induction on t.

The case $t = 1$ follows from Lemma 3.1, so we can assume that $1 < t$. Since M_t has odd index in G_{t-1}, there exists a unique rational-valued $\theta \in \mathrm{Irr}(G_{t-1}|\psi)$, again by Lemma 3.1. Recall that $\theta(1)/\psi(1)$ divides $|G_{t-1} : M_t|$, by Theorem 1.8, and so θ has odd degree. By uniqueness, θ is P-invariant, and in particular θ is invariant in M_{t-1} because $M_{t-1}/G_{t-1} \leq PG_{t-1}/G_{t-1}$. Also, it follows from $\mathbf{O}^2(G_{t-1}) = G_{t-1}$ that θ has odd determinantal order, and thus $o(\theta) = 1$ because θ is real. Therefore, θ has a unique canonical extension $\hat{\theta} \in \mathrm{Irr}(M_{t-1})$, which is P-invariant and rational by uniqueness.

Now, write $\chi_1 = \hat{\theta}$ and $\chi_2 = \lambda_{t-1}\hat{\theta}$, so $\chi_i \in \mathrm{Irr}_{2',\mathbb{Q}}(M_{t-1}|\psi)$ for $i = 1, 2$. Since the characters χ_i are P-invariant, induction applies and we deduce that $\mathrm{Irr}_{2',\mathbb{Q}}(G|\chi_i)$ has size at least 2^{t-2}, for $i = 1, 2$. Notice that χ_1 and χ_2 are not conjugate in G, because $o(\chi_1) \neq o(\chi_2)$. In fact, if $\mathcal{X}$ is a representation of M_{t-1} affording $\chi_1 = \hat{\theta}$ then

$$o(\chi_2) = o(\det(\lambda_{t-1}\mathcal{X})) = o((\lambda_{t-1})^{\hat{\theta}(1)}\det\mathcal{X}) = o(\lambda_{t-1})o(\hat{\theta}),$$

since $o(\lambda_{t-1})$ is a power of 2 and $o(\hat{\theta})\hat{\theta}(1)$ is odd. In particular, no irreducible character of G lies over both χ_i. The claim now follows, given that

$$\mathrm{Irr}_{2',\mathbf{Q}}(G|\chi_i) \subseteq \mathrm{Irr}_{2',\mathbf{Q}}(G|\psi).$$

Finally, since P fixes the non-trivial characters $\lambda_t \in \mathrm{Irr}_{2',\mathbf{Q}}(M_t)$, and the sets $\mathrm{Irr}_{2',\mathbf{Q}}(G|\lambda_t)$ are disjoint for different values of $1 \leq t \leq l$, the claim implies that

$$|\mathrm{Irr}_{2',\mathbf{Q}}(G)| > |\mathrm{Irr}_{2',\mathbf{Q}}(G|\lambda_1)|+|\mathrm{Irr}_{2',\mathbf{Q}}(G|\lambda_2)|+\cdots+|\mathrm{Irr}_{2',\mathbf{Q}}(G|\lambda_l)| \geq 1+2+\cdots+2^{l-1} = 2^l-1,$$

where first inequality is strict because the principal character $1_G \in \mathrm{Irr}_{2',\mathbf{Q}}(G)$ does not lie over any character λ_t. The proof is complete. ▮

3.3 Generalization

As Theorem B illustrates, the prime number 2 plays an important role when it comes to control the odd-degree rational characters of a finite group. In order to understand better this relationship, it may be helpful to think on the easiest case treated in Theorem B for a moment. In fact, observe that a non-trivial 2-group always has a non-trivial rational irreducible character of odd degree. With this in mind, it may seem natural to consider the field $\mathbb{Q}_p = \mathbb{Q}(\xi)$, where $\xi \in \mathbb{C}$ is a primitive pth root of unity, as a candidate to substitute the field of rational numbers in results of the type of Theorem B, for an arbitrary prime p. Of course, here we are appealing to the fact that any non-trivial p-group P has a non-trivial p'-degree irreducible character with values in $\mathbb{Q}_p$, as any irreducible character of $P/\Phi(P)$ lies in $\mathrm{Irr}_{p',\mathbb{Q}_p}(P)$.

The main result in this section is a generalization of Theorem B to arbitrary prime numbers. It can be proved using similar arguments to those in the proof of Theorem B, but now we shall use Isaacs canonical set of characters $B_p(G)$ (see Section 1.5). We recall that by Theorem 1.15, the set $B_p(G)$ is invariant under the action of the Galois group $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$. Also, note that the definition of p-length of a solvable group given before is valid for p-solvable groups in general.

Theorem 3.4. *Let G be a p-solvable group of p-length l. Then $\mathrm{Irr}_{p',\mathbb{Q}_p}(G)$ has size at least 2^l.*

Proof. It is clear that we can assume that p divides the order of G, since the principal character of G lies in $\mathrm{Irr}_{p',\mathbb{Q}_p}(G)$. We shall use the same notation as in the definition of the p-length of G for the characteristic subgroups M_t, G_t of G.

Let P be a Sylow p-subgroup of G. We let P act by conjugation on the set of linear characters of M_t/G_t which have values in $\mathbb{Q}_p$, for every $1 \leq t \leq l$. This set consists precisely of those characters of M_t/G_t that contain the Frattini subgroup $\Phi(M_t/G_t)$ in the kernel. Since M_t/G_t is a non-trivial p-group, the number of such characters is a non-trivial power of p, for each t. Of course, the trivial character 1_{M_t} is invariant under the

action of P, and it follows that P fixes a non-trivial linear character $\lambda_t \in \mathrm{Irr}(M_t/G_t)$ which has values in $\mathbb{Q}_p$, for each $1 \leq t \leq l$. It easily follows from the definition of B_p-characters that $\lambda_t \in B_p(M_t)$, for each t (or alternatively because $1_{G_t} \in B_p(G_t)$ and M_t/G_t is a p-group).

Let $\psi \in \mathrm{Irr}_{p',\mathbb{Q}_p}(M_t)$ be P-invariant and assume that ψ is a B_p-character, for some $1 \leq t \leq l$. We claim that the number of characters in $B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G|\psi)$ is at least 2^{t-1}, for $1 \leq t \leq l$. We proceed by induction on t.

The case $t = 1$ follows from Theorem 1.20, so we can assume that $1 < t$. Again by Theorem 1.20, there exists a unique character in $B_p(G_{t-1})$ lying over ψ. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_p)$, so θ^σ is a B_p-character of G_{t-1} lying over $\psi^\sigma = \psi$. By uniqueness of θ, it follows that $\theta^\sigma = \theta$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_p)$, and therefore $\mathbb{Q}(\theta) \subseteq \mathbb{Q}_p$, by basic Galois theory. Also, using similar arguments we deduce that θ is invariant under the action of P, because ψ is P-invariant.

It is now clear that θ is invariant in M_{t-1} because $M_{t-1}/G_{t-1} \leq PG_{t-1}/G_{t-1}$. Also, it follows from $\mathbf{O}^p(G_{t-1}) = G_{t-1}$ that θ has determinantal order coprime to p. Therefore, θ has a unique canonical extension $\hat{\theta} \in \mathrm{Irr}(M_{t-1})$, which is P-invariant and satisfies $\mathbb{Q}(\hat{\theta}) = \mathbb{Q}(\theta)$, by uniqueness (see Theorem 1.11 and the comments before Corollary 2.6).

Now, write $\chi_1 = \hat{\theta}$ and $\chi_2 = \lambda_{t-1}\hat{\theta}$, so $\chi_i \in \mathrm{Irr}_{p',\mathbb{Q}_p}(M_{t-1}|\psi)$ for $i = 1, 2$. By Theorem 1.19, $\chi_i \in B_p(M_{t-1})$ since θ is a B_p-character. Also, since the characters χ_i are P-invariant, induction applies and we deduce that the size of $B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G|\chi_i)$ is at least 2^{t-2}, for $i = 1, 2$. Notice that χ_1 and χ_2 are not conjugate in G, because $o(\chi_1)$ is coprime to p, while p divides $o(\chi_2) = o(\lambda_{t-1})o(\hat{\theta})$, arguing as in the case $p = 2$. In particular, no irreducible character of G lies over both χ_i.

Finally, since P fixes the non-trivial characters $\lambda_t \in B_p(M_t) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(M_t)$, and the sets $\mathrm{Irr}_{p',\mathbb{Q}_p}(G|\lambda_t)$ are disjoint for different values of $1 \leq t \leq l$, the claim implies that

$$|B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G)| > |B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G|\lambda_1)| + \cdots + |B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G|\lambda_l)| \geq$$

$$\geq 1 + 2 + \cdots + 2^{l-1} = 2^l - 1,$$

where the first inequality is strict because the principal character $1_G \in B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G)$ does not lie over any character λ_t. ∎

The following was pointed out to us by J. Sangroniz.

Remark 3.5. It is possible to improve the bound in Theorem 3.4 when p is an odd prime, by showing that $|\mathrm{Irr}_{p',\mathbb{Q}_p}(G)| > 2^l$, with the same notation as in the theorem. Observe that if G/M_1 has even order, then it has a non-principal rational-valued linear character μ. Of course, $\mu \in \mathrm{Irr}_{p',\mathbb{Q}_p}(G)$ and μ has not been computed in the proof of Theorem 3.4, so we are done in this case. Assume now that G/M_1 has odd order. We claim that this implies that λ_1 is not conjugate to λ_1^{-1} in G, using the notation in the proof of Theorem 3.4. To see this, note that if ${\lambda_1}^g = \lambda_1^{-1}$ for some $g \in G$ with $o(gM_1) = n$, then $\lambda_1 = {\lambda_1}^{g^n} = \lambda_1^{-n} = \lambda_1^{-1}$, which contradicts the fact that $o(\lambda_1) = p$ is odd. In particular, no irreducible character of G lies over both λ_1 and λ_1^{-1}. By the arguments in the proof of Theorem 3.4, there exists $\chi \in \mathrm{Irr}_{p',\mathbb{Q}_p}(G|\lambda_1^{-1})$, and χ has not been counted before.

Therefore in any case we have that $|\mathrm{Irr}_{p',\mathbb{Q}_p}(G)| > 2^l$, as wanted. We observe that if G/M_1 has even order, the character μ does not lie in $B_p(G)$. ▮

It is clear from the proof of the previous theorem, that in fact the number characters in $\mathrm{Irr}_{p',\mathbb{Q}_p}(G) \cap B_p(G)$ is at least 2^l, using the same notation. Let us write $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$, and recall that this Galois group acts naturally on the set of characters of G with values contained in $\mathbb{Q}_p$. Also, this action preserves degrees of characters, and thus $\mathcal{G}$ permutes the set $\mathrm{Irr}_{p',\mathbb{Q}_p}(G)$. In particular, $\mathcal{G}$ also permutes the B_p-characters lying in $\mathrm{Irr}_{p',\mathbb{Q}_p}(G)$. Observe that since $\mathrm{Aut}(G)$ acts naturally on $B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G)$, then $\mathrm{Aut}(G) \times \mathcal{G}$ permutes this set of characters aswell.

Suppose that χ, φ are two distinct characters of a p-solvable group G lying in $B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G|\lambda_t)$ with $t > 1$, and that they are like the ones constructed in the proof of Theorem 3.4. Using the same notation as in the proof of Theorem 3.4, the restrictions of χ and φ to some M_j, with $j \leq t-1$, have irreducible constituents with distinct determinantal order, and this implies that χ and φ do not lie in the same $\mathrm{Aut}(G) \times \mathcal{G}$-orbit. Thus, if G has p-lenght l, then the action of $\mathrm{Aut}(G) \times \mathcal{G}$ on $B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G)$ has at least 2^l orbits.

3.4 Some Consequences

In this section, we collect some consequences of the main results in this chapter.

We start by presenting a new local/global relationship which is a consequence of Theorem B. Suppose that G is a solvable group, and let P be a Sylow 2-subgroup of G. Also, write $N = \mathbf{N}_G(P)$ for the normalizer of P in G. Then conjugation defines a natural action of N on $P/\Phi(P)$, given that $\Phi(P) \lhd N$. Next result is due to P. Centella and G. Navarro.

Lemma 3.6. *Let G be a solvable group, $P \in \mathrm{Syl}_2(G)$ and $N = \mathbf{N}_G(P)$. Then the number of odd-degree irreducible rational characters of G is the number of N-orbits on $P/\Phi(P)$.*

Proof. See Corollary B of [4]. ▮

Therefore, we have the following application of Theorem B.

Corollary 3.7. *Let G be a solvable group of 2-length $l \in \mathbb{N}$. Suppose that $P \in \mathrm{Syl}_2(G)$, and let N be the normalizer of P in G. Then the number of N-orbits on $P/\Phi(P)$ is at least 2^l.*

We next explain another interesting consequence of Theorem B. A celebrated result of J. Thompson (see IX.8.6 of [12]) states that if G is a solvable group with a unique conjugacy class of involutions, and a Sylow 2-subgroup of G contains more that one involution, then G has 2-length one.

Observe that Thompson's theorem easily implies that a solvable group G with two rational conjugacy classes has 2-length one. To see this, we can assume that a Sylow 2-subgroup P of G is not cyclic, since otherwise G has a normal 2-complement (see Theorem 2.1). Also, P is not a -generalized- quaternion 2-group, because in that case P would have

a rational element of order four, and we would obtain at least three rational classes, against our assumption (of course, the class of the identity element and the class of involutions are rational). Now, since cyclic and quaternion 2-groups are the only 2-groups with a unique involution, our claim follows.

The result discussed in the previous paragraph was improved by M. Isaacs and G. Navarro in [18], where they proved that a solvable group with at most three rational conjugacy classes has 2-length at most one. Following [18], the problem can be reduced to show that a solvable group G with at most three real-valued characters lying in $B_2(G)$ has 2-length one. Then, a possible way to complete the proof is to notice that a real irreducible character of odd degree of G always lies in $B_2(G)$. So a direct application of Theorem B gives the desired theorem.

To close this section, we show that odd primes have a better behavior that the prime 2 in the situation above described. In fact, the following is an immediate consequence of Theorem 3.4. Again, we make use of basic results about B_p-characters.

Theorem 3.8. *Let G be a p-solvable group of p-length l, where p is an odd prime. Then the number of orbits of $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$ on the conjugacy classes of p-elements of G with values in $\mathbb{Q}_p$ is at least 2^l.*

Proof. Write $|G|_p = p^a$. We know that every character in $B_p(G)$ has its values in $\mathbb{Q}_{p^a}$ by Theorem 1.16, and thus $\mathcal{H} = \mathrm{Gal}(\mathbb{Q}_{p^a}/\mathbb{Q})$ acts on $B_p(G)$. Then, $\mathcal{H}$ also acts on $B_p(G) \cap \mathrm{Irr}_{\mathbb{Q}_p}(G)$, and $\mathcal{H}$ partitions this set into exactly the same orbits as the action of $\mathcal{G}$ on it, by elementary Galois theory. By the proof of Theorem 3.4 (see the comments after the proof), we have that the number of orbits of $\mathcal{H}$ on $B_p(G)$ is at least 2^l.

Consider now the matrix

$$M = (\chi(g)),$$

where $\chi \in B_p(G)$ and x runs over a set of representatives of the conjugacy classes of p-elements of G. By Theorem 1.17 M is an invertible square matrix. Of course, $\mathcal{H}$ permutes the conjugacy classes of p-elements of G, as well as the characters in $B_p(G)$. By Brauer's Theorem 1.18, the actions of the cyclic group $\mathcal{H}$ on these sets of characters and conjugacy classes are permutation isomorphic. In particular, the subgroup $\mathrm{Gal}(\mathbb{Q}_{p^a}/\mathbb{Q}_p)$ of $\mathcal{H}$ fixes the same number of B_p-characters and conjugacy classes of p-elements of G.

The result now follows, since the B_p-characters of G fixed by $\mathrm{Gal}(\mathbb{Q}_{p^a}/\mathbb{Q}_p)$ are precisely those with field values contained in $\mathbb{Q}_p$, by basic Galois theory, and the same holds for conjugacy classes of p-elements. ∎

3.5 Some Examples

In this section we present examples of p-solvable groups attaining some of the bounds proved in the chapter. We thank J. Sangroniz for suggesting more general versions of our original examples, and also for significantly improving the way of presenting them.

We start by defining a sequence of solvable groups $G_1, G_2, \ldots$ such that for every $l \in \mathbb{N}$, the group G_l has 2-length l and precisely 2^l rational characters of odd degree. As a consequence, we deduce that the bound in Theorem B cannot be improved.

Let A be a group of permutations on n symbols, and assume that the Sylow p-subgroups of A are transitive. Let H be any group, and consider the corresponding wreath product $G = H \wr A$. Let $\chi \in \mathrm{Irr}_{p',\mathbb{Q}_p}(G)$ and let $\psi \in \mathrm{Irr}(B)$ be an irreducible constituent of χ_B, where $B \leq G$ is the base group of the wreath product. Since B is isomorphic to n copies of H, we have that

$$\psi = \delta_1 \times \cdots \times \delta_n ,$$

where $\delta_i \in \mathrm{Irr}(H)$. Let T be the inertia group of ψ in G, so $\chi = \eta^G$ for some $\eta \in \mathrm{Irr}(T|\delta)$, by Clifford's Correspondence. Since $\chi(1)$ is not divisible by p, it follows that $|G : T|$ is not divisible by p, by the induction formula. It is clear that $T = B(T \cap A)$, and thus $|A : T \cap A| = |G : T|$ is coprime to p. Therefore $A \cap T$ contains a Sylow p-subgroup of T, and we have that $A \cap T$ acts transitively on the direct factors of the base group B. Observe that if $\sigma \in T \cap A$, then

$$\delta_1 \times \cdots \times \delta_n = (\delta_1 \times \cdots \times \delta_n)^\sigma = \delta_{\sigma(1)} \times \cdots \times \delta_{\sigma(n)} ,$$

so $\delta_i = \delta_{\sigma(i)}$ for all $1 \leq i \leq n$. Now, since $T \cap A$ is transitive, we deduce that

$$\delta_1 = \cdots = \delta_n = \delta .$$

It then follows that ψ is invariant in G, i. e. $T = G$ and $\chi_B = e\psi$ for some positive integer e, by Clifford's Theorem 1.7. In particular, we deduce that ψ is lies in $\mathrm{Irr}_{p',\mathbb{Q}_p}(H)$. Next we can use the following well-known result by S. Mattarei.

Lemma 3.9. *Let A be a permutation group and H any group. Let $G = H \wr A$ be the wreath product, and write $B \leq G$ for the base group of G. If $\psi \in \mathrm{Irr}(B)$ is invariant in G, then ψ has an irreducible extension to G which has the same field of values as ψ.*

Proof. See Lemma 1.3 of [25]. ∎

By Lemma 3.9, we can assume that $\chi_0 \in \mathrm{Irr}(G)$ is an extension of ψ having the same field of values as ψ. By Gallagher's Theorem 1.10, the characters in $\mathrm{Irr}(G|\psi)$ are precisely those that can be (uniquely) written as $\beta\chi_0$, where $\beta \in \mathrm{Irr}(G/B)$. If $\beta \in \mathrm{Irr}(G/B)$, then $\beta\chi_0$ has its values in $\mathbb{Q}_p$ if and only if

$$\beta\chi_0 = (\beta\chi_0)^\tau = \beta^\tau\chi_0$$

for all $\tau \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$, which is equivalent to say that $\beta^\tau = \beta$ for all such τ, by uniqueness in Gallagher's result. Then $\beta\chi_0$ has its values in $\mathbb{Q}_p$ if and only if $\mathbb{Q}(\beta) \subseteq \mathbb{Q}_p$, by Galois theory. Therefore, since $A \cong G/B$, we conclude that $|\mathrm{Irr}_{p',\mathbb{Q}_p}(G|\psi)| = |\mathrm{Irr}_{p',\mathbb{Q}_p}(A)|$ and thus

$$|\mathrm{Irr}_{p',\mathbb{Q}_p}(G)| = |\mathrm{Irr}_{p',\mathbb{Q}_p}(H)|\,|\mathrm{Irr}_{p',\mathbb{Q}_p}(A)| .$$

We can now iterate the above construction. If A is a subgroup of the symmetric group on n symbols whose Sylow p-subgroups are transitive, define $G_1 = A$, $G_l = G_{l-1} \wr A$ for $l > 1$. Then $|\mathrm{Irr}_{p',\mathbb{Q}_p}(G_l)| = |\mathrm{Irr}_{p',\mathbb{Q}_p}(A)|^l$. In particular, note that if $A = A_4$ (and $p = 2$) then G_l has 2^l rational irreducible characters of odd degree, because $|\mathrm{Irr}_{2',\mathbb{Q}}(A)| = 2$.

In order to compute the p-length of the groups G_l just constructed, we can appeal to the following result by P. Hall and G. Higman on the p-length of wreath products, which is not very difficult to prove:

Lemma 3.10 (Hall-Higman). *Let A be a permutation group on n symbols and H any group. Suppose that both A and H are p-solvable and that they have p-length l_1 and l_2, respectively. If $\mathbf{O}^p(H) = H$, then the wreath product $H \wr A$ has p-length $l_1 + l_2$.*

Proof. See Lemma 3.5.1 of [11]. ▮

Continuing to assume that $A = A_4$ and $G_1 = A$, $G_l = G_{l-1} \wr A$ for $l > 1$, we have that $\mathbf{O}^2(A) = A$, and thus it is immediate that $\mathbf{O}^2(G_l) = G_l$. In particular, we deduce from Lemma 3.10 that G_l has 2-length l for all $l \geq 1$, since A has 2-length 1. Consequently, the bound in Theorem B cannot be improved.

The above construction can also be used to obtain examples for odd prime numbers. Next we show that for any natural number l, there exists a p-solvable group J_l whose p-length is p and such that $|B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(J_l)| = 2^l$, where p is any odd prime. (This implies that the bound obtained in the proof of Theorem 3.4 is sharp.)

Suppose that A is a permutation group on n symbols which has a non-trivial normal Sylow p-subgroup P, and assume that P is transitive. Suppose also that A/P acts transitively on the non-trivial characters of P/P', and let H be any finite group with $\mathbf{O}^p(H) = H$. As before, write $G = H \wr A$ for the wreath product, and let $B \leq G$ be the base group. Also, write K/B for the unique Sylow p-subgroup of G/B.

Let $\chi \in B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G)$ and $\psi \in \mathrm{Irr}(B)$ an irreducible constituent of χ_B. Arguing as before, we have that $\psi \in \mathrm{Irr}_{p',\mathbb{Q}_p}(B)$ and ψ is invariant in G. Also, ψ is a B_p-character by Theorem 1.21, because $\chi \in B_p(G)$. Observe that if $\chi_0 \in B_p(G|\psi)$ then the irreducible constituents of $(\chi_0)_K$ are G-conjugate B_p-characters of K lying over ψ, by Theorem 1.7 and Theorem 1.21, using the fact that ψ is invariant in G. Also, if $\theta_0 \in B_p(K|\psi)$ then there exists a unique character in $B_p(G|\psi)$ lying over θ_0, by Theorem 1.20, and this unique character also lies over $(\theta_0)^g$ for all $g \in G$. By Theorem 1.7 and Theorem 1.8, a character $\chi_0 \in \mathrm{Irr}(G)$ has p'-degree if and only if $\theta_0 \in \mathrm{Irr}(K)$ has p'-degree, where $[\chi_0, \theta_0] \neq 0$. It is now clear that the size of $B_p(G) \cap \mathrm{Irr}_{p'}(G|\psi)$ equals the number of G-orbits of p'-degree B_p-characters of K lying over ψ.

Observe that since $\mathbf{O}^p(B) = B$, there exists a unique canonical extension $\hat{\psi} \in \mathrm{Irr}(K)$ of ψ, and $\hat{\psi}$ is a B_p-character by Theorem 1.19. By Gallagher's Theorem 1.10 and Theorem 1.19, the p'-degree B_p-characters of K lying over ψ are precisely the characters $\beta\hat{\psi}$, where β is any linear character of K/B. By hypothesis, G acts transitively on the non-principal linear characters of K/B, and thus G partitions the set $B_p(K) \cap \mathrm{Irr}_{p'}(K)$ into two orbits, given that $\hat{\psi}$ is G-invariant. In particular, there are two B_p-characters of p'-degree of G lying over ψ. One of them lies over $\hat{\psi}$ and the other one lies over $\beta\hat{\psi}$, where β is as before and non-principal. Since G acts transitively on the non-principal characters of P/P', it is clear that $\mathbb{Q}(\beta) \subseteq \mathbb{Q}_p$. Now, for all $\tau \in \mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$ we have that $\hat{\psi}^\tau = \hat{\psi}$ by uniqueness of the canonical extension, and thus $(\beta\hat{\psi})^\tau = \beta\hat{\psi}$. In particular, the two B_p-characters of G having p'-degree and lying over ψ have values in $\mathbb{Q}_p$, by routine arguments.

We deduce from the two previous paragraphs that

$$|B_p(G) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(G)| = 2\,|B_p(H) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(H)|\,.$$

Now, if we write $J_1 = A$ and $J_l = J_{l-1} \wr A$ for $l > 1$, we have that

$$|B_p(J_l) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(J_l)| = 2^{l-1} |B_p(A) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(A)| .$$

Bearing in mind that A has a normal Sylow p-subgroup P and that A/P acts transitively on the non-principal linear characters of P, it is not difficult to check that A has precisely two B_p-characters of p'-degree with values in $\mathbb{Q}_p$, and we deduce that

$$|B_p(J_l) \cap \mathrm{Irr}_{p',\mathbb{Q}_p}(J_l)| = 2^l,$$

for $l > 1$. Notice that $\mathbf{O}^p(A) = A$, so J_l has p-length l by Lemma 3.10. In particular, if $A = C_p \rtimes C_{p-1}$, where C_s is the cyclic group of order s, then J_l is as desired.

Finally, we include an example which was kindly provided to us by J. Sangroniz. Let $A = AGL(1, \mathbb{Z}_p)$ be the affine group over $\mathbb{Z}_p$. Then A can be viewed as a subgroup of the symmetric group on p symbols, and its Sylow p-subgroup is transitive. Also, $\mathbf{O}^p(A) = A$, A has p-length 1 and the number of irreducible characters of A of p'-degree with values in $\mathbb{Q}_p$ equals 3. Then, the usual iterated construction leads to a sequence of solvable groups $G_1, G_2, \ldots$ with $|\mathrm{Irr}_{p',\mathbb{Q}_p}(G_l)| = 3^l$ and such that G_l has p-length l for all $l \geq 1$.

Chapter 4

2-Groups with few rational conjugacy classes

4.1 Introduction

Finite groups of order a power of two and maximal nilpotence class (see Section 4.2 for a definition) appear naturally in many different situations within group theory. Probably the first observation that we should make about this family of groups is that it is infinite, since for any power of two bigger than four, there exist groups of maximal class having that cardinality, although not many. Indeed, the only non-abelian groups of order eight are the quaternion group and the dihedral group, and for any bigger power of 2 there are exactly three isomorphism types of groups of maximal class having that order. Of course, these groups are the dihedral, semi-dihedral and generalized quaternion 2-groups (see Theorem 4.1 below).

Let us recall that dihedral, semi-dihedral and generalized quaternion 2-groups admit several well-known characterizations which can be considered as standard results; for some examples, we refer to Section 4.2 below. A more recent result of this type [20] was first conjectured by G. Navarro, and it is of particular of interest to us, because it deals with rationality in finite groups. It is an easy exercise to check that 2-groups of maximal class have precisely 5 rational irreducible characters, and the authors in [20] showed that in fact this condition is necessary and sufficient.

Since dihedral, semi-dihedral and generalized quaternion 2-groups possess exactly 5 rational conjugacy classes, it seems natural to expect that this condition also characterizes the maximal class 2-groups, as was conjectured by G. Navarro as well. In this chapter, we prove that this is actually the case, and that is the main result in the chapter.

Theorem C. *Let G be a 2-group with 5 conjugacy classes of rational elements. Then G is either a dihedral, semi-dihedral or generalized quaternion group.*

In [20], the first step to prove that 2-groups with five irreducible rational characters have maximal class is to determine the 2-groups with four irreducible rational characters. In this chapter, we shall also characterize the 2-groups with exactly four conjugacy classes of rational elements, but Theorem C above is independent of this result. In particular, we shall see that although all 2-groups with four rational irreducible characters have four rational classes, the converse is not true.

As it is straightforward to check for rational characters, we shall see that there are no 2-groups with precisely three rational classes. However, the proof of this result on conjugacy classes is not completely trivial, and in fact it probably serves as an illustration of the difference between our techniques and those used in [20]. When dealing with rational characters, sometimes it is certainly convenient to consider quotient groups, since characters of a quotient group are characters of the whole group. By contrast, a rational class in a quotient group does not necessarily come from a rational class in the whole group. To compensate, rational elements in a subgroup are also rational in the whole group.

In Section 4.2, some preliminary results are presented, and among other facts a classification of metacyclic 2-groups according to their number of rational conjugacy classes is included. As we shall see, it follows from this classification that the result in Theorem C holds for metacyclic 2-groups; observe that it is then enough to show that 2-groups with 5 conjugacy classes of rational elements are metacyclic, in order to deduce Theorem C in all its generality. This last step in the proof of Theorem C is left for the final section of the chapter, where the announced characterization of 2-groups with four rational classes is completed aswell.

The results in this chapter are joint work by the author and Josu Sangroniz, and have been published in [32].

4.2 Preliminary Results

Let G be a finite group, and define the normal subgroups Z_i of G, for $i \geq 0$, as follows. Let $Z_0 = 1$, and $Z_i/Z_{i-1} = \mathbf{Z}(G/Z_{i-1})$ for $i > 0$. Then the series

$$1 = Z_0 \leq Z_1 \leq \cdots \leq Z_i \leq \cdots \leq G$$

is called the **upper central series** of G. The group G is nilpotent if and only if there exists an integer l such that $Z_l = G$, and in this case the minimal integer satisfying this is the **nilpotence class** of G. Of course, a group G is nilpotent of class one if and only if G is abelian.

It is clear that a finite p-group G of order p^s is nilpotent and its class is at most $s-1$. If it is $s-1$, then we say that G has **maximal class**.

The following result is fairly well-known.

Theorem 4.1. *A finite 2-group G has maximal nilpotence class if and only if G is either dihedral, semi-dihedral or generalized quaternion.*

Proof. See Theorem III 11.9(b) of [12]. ∎

Let us next recall the basic fact that cyclic and generalized quaternion 2-groups are the only 2-groups having a unique involution.

Theorem 4.2. *Let G be a p-group containing at most one subgroup of order p, where p is a prime. Then either G is cyclic, or else $p = 2$ and G is generalized quaternion.*

Proof. See Theorem 6.11 of [14]. ∎

Since we are studying 2-groups with few rational conjugacy classes, results aimed to locate rational elements in these groups are of obvious interest. We have a couple of lemmas of this type. If G is a 2-group, we denote the subgroup generated by the involutions of G by $\Omega_1(G)$, and $\Omega_2(G)$ is the subgroup generated by the elements of order at most 4. Also, G^2 denotes the subgroup of G generated by the squares of the elements of G.

Lemma 4.3. *Let G be a 2-group and K an abelian normal subgroup of rank 2 which is not elementary abelian. Suppose that $\Omega_1(K)$ is not contained in the center of G. Then G has rational elements of order 4 lying in K.*

Proof. We can assume without loss of generality that $K \cong C_2 \times C_4$. Then the subgroup K^2 is cyclic of order 2 and normal in G, so it is central. Let z be a generator of it and $g \in G \setminus \mathbf{C}_G(\Omega_1(K))$. Since K is generated by its elements of order 4, g does not commute with some $x \in K$ of order 4 and we claim that x is rational in G. This is clear if g normalizes $\langle x \rangle$. Otherwise $x^g = xu$ for some non-central involution u in K, so $u^g = uz$ and, as $x^2 = z$, $x^{g^2} = xz = x^{-1}$. ∎

Before disposing of the other lemma, as an application of the last result we prove that a 2-group cannot have exactly 3 rational conjugacy classes.

Theorem 4.4. *Let G be a finite 2-group. Then $|\mathrm{Cl}_{\mathbb{Q}}(G)| \neq 3$.*

Proof. Suppose that G has 3 rational conjugacy classes. Then G has only one central involution z, because abelian 2-groups of rank bigger than one have at least 3 involutions. Since a 2-group with exactly one involution is either cyclic or generalized quaternion by Theorem 4.2, and none of these groups has 3 rational classes (see the proof of Lemma 2.18), it follows that G must have a non-central class of involutions. Then the classes containing involutions and the class of the identity in G amount to all the rational classes of G. In particular, G cannot have any rational element of order 4.

Following with the same notation, observe that if u is a non-central involution, then u must commute with any other involution, since two non-commuting involutions generate a dihedral 2-group (see Lemma 2.14 of [14]), and dihedral 2-groups have rational elements of order 4 (see the proof of Lemma 2.18). Thus $L = \Omega_1(G)$ is elementary abelian and is the union of $\langle z \rangle$ and the class of u. By counting elements, it is clear that $|L| = 4$. Observe that if L is self-centralizing in G, then $|G| \leq 8$ because $\mathrm{Aut}(L)$ has size 6; but this is impossible, and then we have that $L < \mathbf{C}_G(L)$. In particular, there exists a normal subgroup K isomorphic to $C_2 \times C_4$ containing L, and we can use last lemma to produce a rational element of order 4 in K, obtaining the desired contradiction. ∎

Lemma 4.5. *Let G be a 2-group with a unique conjugacy class of rational elements of order 4, and suppose that $N = \Omega_1(G) \subseteq \mathbf{Z}(G)$. Then, if x is a rational element of order 4, we have that $\langle x \rangle N$ is a normal subgroup of G.*

Proof. It suffices to show that if $y \in G$ is conjugate to x, then xy has order at most 2 (so that $xy \in N$ and $y \in \langle x \rangle N$).

Suppose then that $y = x^g$. Then

$$(x^{-1}y)^x = x^{-2}x^g x = (x^{-1})^g x = y^{-1}x = (x^{-1}y)^{-1}$$

(in the second equality we have used that $x^2 \in N \subseteq \mathbf{Z}(G)$). If xy has order greater that 2 so does $x^{-1}y = [x, g]$ and a power of this commutator would be rational of order 4. Since G is nilpotent, there exists an integer $i \geq 1$ such that $x \in Z_i \setminus Z_{i-1}$, and thus $[x, g] \in [Z_i, G] \leq Z_{i-1}$. This implies that no power of $[x, g]$ is conjugate to x in G, because $Z_{i-1} \lhd G$, and this contradiction proves the result. ∎

Next, we include -without proof- some known results that we shall need later in this chapter. The following characterizations of the maximal class 2-groups are indeed well-known; we remark that in the situation of Theorem C, the next theorem is particularly convenient, given that a restriction on the number of involutions in a group with few rational classes is usually a strong condition.

Theorem 4.6 (Alperin-Feit-Thompson). *Let G be a 2-group containing exactly t involutions. If $t \equiv 1 \bmod 4$, then either G is cyclic or $|G : G'| = 4$.*

Proof. See Theorem 4.9 of [13]. ∎

Of course, Theorem 4.6 is a result about 2-groups of maximal class because of next theorem, due to O. Taussky.

Theorem 4.7 (Taussky). *Let G be a non-abelian 2-group with $|G : G'| = 4$. Then G has maximal nilpotence class.*

Proof. See Theorem III 11.9(a) in [12]. ∎

Conversely, recall that if G is a dihedral, semidihedral or generalized quaternion 2-group then $|G : G'| = 4$, and the number of involutions of G is congruent to 1 mod 4, as it is easy to check (see the proof of Lemma 2.18 for a brief description of the rational classes and rational characters of maximal class 2-groups).

Recall that a group G is **metacyclic** if there exists a cyclic normal subgroup N of G such that G/N is cyclic.

Theorem 4.8 (Isaacs-Navarro-Sangroniz). *Let G be a non-abelian 2-group with 4 or 5 rational irreducible characters. Then G is metacyclic.*

Proof. See Theorem A and Theorem F of [20]. ∎

Observe that the last theorem can be used to show that a (non-abelian) 2-group G with 5 real irreducible characters is metacyclic. In fact, note that G is not cyclic, and thus $|G/\Phi(G)| > 2$. Since the characters of $G/\Phi(G)$ are precisely the linear real-valued characters of G, we have that $|G/\Phi(G)| = 4$ and hence G has exactly one non-linear real character. Also, all linear real characters of G are rational. Since Galois automorphisms preserve degrees of characters and fields of values, the unique non-linear real irreducible character χ of G is fixed by all $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$, and so χ is rational-valued. In particular, G has 5 rational irreducible characters, and we can apply Theorem 4.8.

4.2.1 Metacyclic Groups

We can now prove that the result in Theorem C is true for metacyclic 2-groups. More precisely, we classify metacyclic 2-groups into 4 different families, and then count the rational conjugacy classes of the groups in each class. From this, we deduce that metacyclic 2-groups with 5 rational conjugacy classes have maximal nilpotence class. We need the following easy number theoretic lemma.

Lemma 4.9. *Let $n \geq 8$ be power of 2 and k an odd integer whose residue class module n has order $m \geq 4$ in the multiplicative group of units of $\mathbb{Z}_n$. Then $2n$ does not divide $k^m - 1$, i. e. k has not order m in the group of units of $\mathbb{Z}_{2n}$.*

Proof. Let $U(n)$ be the group of units of the ring $\mathbb{Z}_n$. As is well-known, $U(n) \cong C_2 \times C_{n/4}$ (see Theorem 4.10 of [22], for instance). The residue class of 5 in $\mathbb{Z}_n$ has order $n/4$ in $U(n)$, and -1 generates the complementary group C_2. The involutions in $U(n)$ are (the classes of) $n-1$, $n/2-1$ and $n/2+1$. Observe that since $5^{n/8} \equiv n/2+1 \pmod{n}$, the class of $n/2+1$ is the unique involution in $U(n)$ that is a square. In particular $k^{m/2} \equiv n/2+1 \pmod{n}$. Since $n/2+1$ has order 4 in $U(2n)$, the result follows. ∎

Proposition 4.10. *Let $G = \langle a, b \,|\, a^n = 1, b^m = 1, a^b = a^k$ for some integer $k\rangle$ be a non-abelian metacyclic 2-group. Then the presentation can be chosen so that one of the following conditions holds:*

1. $k \equiv 1 \pmod{4}$.
2. $k \equiv -1 \pmod{4}$, $n, m \geq 8$, $k^{m/4} \equiv 1 \pmod{n}$ *and* $a^{n/2} = b^{m/2}$.
3. *G is of maximal class.*
4. $k \equiv -1 \pmod{4}$, $m \geq 4$ *and* $\langle a\rangle \cap \langle b\rangle = 1$.

Proof. Let a and b be generators of G of order n and m, respectively, and assume that $a^b = a^k$. Suppose that non of the cases 1, 2, 4 holds. In particular, note that $k \equiv -1 \pmod{4}$.

Suppose firts that $\langle a\rangle \cap \langle b\rangle = 1$. Since G does not admit a presentation as in 4, it follows that $m = 2$. Then G is either dihedral or semidihedral and case 3 holds, which is a contradiction. Thus, we have that $\langle a\rangle \cap \langle b\rangle$ is non-trivial, so $a^{n/2} = b^{m/2}$. Observe that $k \equiv -1 \pmod{4}$ implies that the above intersection has size 2. We distinguish the following four cases:

If $n = 4$ and $m = 4$, then G is a generalized quaternion and 3 holds, which is impossible.

If $n = 4$ and $m \geq 8$, then $b^a = b^{1+m/2}$ and we are in case 1 with diffirent generators, a contradiction.

Suppose that $n \geq 8$ and $m = 4$. Since $\langle b\rangle$ induces an automorphism of order 2 on $\langle a\rangle$ and $k \equiv -1 \pmod{4}$, we have that $a^b = a^{-1}$ or $a^b = a^{-1+n/2}$. In the former case G is a generalized quaternion and in the latter, $(ba)^2 = 1$, so G is semidihedral. In any case, G has maximal class, which contradicts our assumption.

Finally, assume that $n, m \geq 8$. Since case 2 does not hold, we have that $k^{m/4} \not\equiv 1 \pmod{4}$. Then k has order $m/2$ in the group of units of $\mathbb{Z}_n$ and, by the last lemma, $2n$

does not divide $k^{m/2}-1$. Now since $(k-1)/2$ is odd, we deduce that $(k^{m/2}-1)(k-1)$ can be written as $sn/2$ for some odd integer s and

$$(ba)^{m/2} = b^{m/2}a^{1+k+\cdots k^{(m/2)-1}} = b^{m/2}a^{(k^{m/2}-1)/(k-1)} = b^{m/2}a^{sn/2} = b^{m/2}a^{n/2} = 1\,.$$

It follows that we are in case 4 taking generators $a' = a$, $b' = ba$. This contradiction proves the result. ∎

Theorem 4.11. *Let G be a non-abelian metacyclic 2-group. Then G has 4 rational conjugacy classes in the cases 1 and 2 in the previous proposition, it has 5 rational classes in the case 3 and 6 rational classes in the case 4.*

Proof. We keep the notation of the preceding proposition. It is an easy exercise to prove that 2-groups of maximal class have exactly 5 rational conjugacy classes so, for the rest of the proof, we shall assume that one of the cases 1, 2 or 4 holds.

We start by showing that G has no rational elements of order greater than 4 except in case 4 when a and $b^{m/2}$ do not commute.

Indeed, if $g \in G$ is a rational element then, as $G/\langle a\rangle$ is abelian, $g^2 \in \langle a\rangle$, whence $\mathbf{N}_G(\langle g^2\rangle)/\mathbf{C}_G(g^2)$ is cyclic. But g^2 is also rational, so $\mathbf{N}_G(\langle g^2\rangle)/\mathbf{C}_G(g^2) \cong \mathrm{Aut}(\langle g^2\rangle)$ and the order of g^2 cannot be greater than 4. Therefore the order of g is at most 8. We suppose that g has order 8. There is no loss if we assume $g^2 = a^{n/4}$. As g^2 is rational, we must have $(g^2)^b = g^{-2}$, so $k \equiv -1 \pmod 4$ and case 1 is ruled out.

If we write $g = b^i a^j$ then $g^2 \in \langle a\rangle$ implies that $b^{2i} \in \langle a\rangle \cap \langle b\rangle$, whence b^i has order at most 4. If the order is 4, then we are in case 2 and b^i is a central element. But then g and a commute, which is impossible because, being g rational, $\mathbf{N}_G(\langle g\rangle)/\mathbf{C}_G(g) \cong \mathrm{Aut}(\langle g\rangle) \cong C_2 \times C_2$, which is not cyclic. So the order of b^i is 2, whence $b^i = b^{m/2}$ and, since we cannot have $b^i \in \langle a\rangle$, case 4 holds. In addition a and $b^{m/2}$ do not commute. Notice that this forces $16 \leq n$. Moreover, as $m/2 \geq 2$, $a^{b^{m/2}} = a^{1+(n/2)}$ and then $a^{n/4} = g^2 = a^{2j}a^{jn/2}$, whence $a^j \in \langle a^{n/8}\rangle$ and $g \in \langle b^{m/2}, a^{n/8}\rangle \cong C_2 \times C_8$. We can check that this subgroup contains a unique rational class of G of elements of order 8, namely the class of $b^{m/2}a^{n/8}$.

Now we work to show that the number of rational classes of elements of order at most 4 is four in cases 1 and 2 and that, in case 4, this number is 6 or 5 according as a and $b^{m/2}$ commute or not, respectively.

A metacyclic 2-group has exactly three involutions except if it is cyclic or of maximal class (see Theorem 2.1 [23]), so we can suppose that $L = \Omega_1(G) \cong C_2 \times C_2$. We denote $x = a^{n/4}$ and $z = x^2$, which is a central involution.

Case 1 is easy: if y is a rational element of order 4, then $y^2 \in \langle a\rangle$ and $y^2 = z$. Since x is central, $u = xy$ is a (non-central) involution whence $y \in \langle u, x\rangle \cong C_2 \times C_4$. Then the rational classes of G are those of 1, z, u and xu. On the other hand, if G has no rational elements of order 4, the three involutions must be central (by aplying Lemma 4.3, for instance) and again G has 4 rational classes.

Case 2 is similar. Of course x is now a rational element of order 4 and $u = xb^{m/4}$ is a (non-central) involution. If y is a rational element of order 4, $(yb^{n/4})^2 = 1$, so

$y \in \langle u, b^{m/4} \rangle = \langle u, x \rangle \cong C_2 \times C_4$. Again G has 4 rational classes (with representatives 1, z, u and x).

Let's consider now the case 4. First, notice that if y is rational of order 4, then it commutes with x for otherwise $x^y = x^{-1}$. This implies that $y = b^i a^j$ with i an odd integer and, working in $G/\langle a \rangle$, we would have that the order of b is the same as the order of $b^i\langle a \rangle = y\langle a \rangle$, which is 2, against the hypothesis $m \geq 4$. Thus xy is an involution and $y \in \langle u, x \rangle \cong C_2 \times C_4$, where $u = b^{m/2}$. Now, if u does not commute with a, there are 5 rational classes inside $\langle u, x \rangle$ (those of 1, z, u, x and xy). On the other hand, if u and a commute, u is central and $\langle u, x \rangle$ is the union of 6 rational classes (those of 1, z, u, zu, x and xu). ∎

According to Theorem F of [21], a non-abelian 2-group G has 4 rational irreducible characters if and only if it contains cyclic subgroups $X \lhd G$ and $Y \leq G$ such that $G = XY$ and $|X \cap \mathbf{Z}(G)| \geq 4$. Observe that these 2-groups are precisely those in the family 1 of Proposition 4.10. However, the groups in the family 2 do have 4 rational conjugacy classes as well. It can be checked that they have 6 rational irreducible characters. It is easy to see that the groups in the family 4 have 6 rational irreducible characters. Also, one can find non-metacyclic 2-groups with 6 rational irreducible characters (for instance, with the help of the GAP software).

It is clear from Theorem 4.11, that in order to proof the main result of this chapter it suffices to show that 2-groups with 5 conjugacy classes of rational elements are metacyclic. Also, observe that if we show that 2-groups with 4 rational classes are metacyclic, then we obtain a characterization of these groups as the groups in the families 1 and 2 in Theorem 4.11.

So the question now is how to prove that 2-groups with few rational classes are metacyclic. To do so, we find it useful a classification of minimal non-metacyclic 2-groups due to N. Blackburn. Recall that a minimal non-metacyclic group is a non-metacyclic group all whose proper subgroups are metacyclic. N. Blackburn found that there are only four isomorphism types of minimal non-metacyclic 2-groups: the elementary abelian group of order 8, $C_2 \times C_4$, the central product $Q_8 * C_4$ of order 16 and the group with presentation $\langle a, b, c, |a^4 = b^4 = [a, b] = 1, c^2 = a^2, a^c = ab^2, b^c = ba^2 \rangle$ (see [1], Theorem 66.1; indeed, N. Blackburn also classified the minimal non-metacyclic p-groups for p an odd prime, but we shall not need that result).

Observe that all minimal non-metacyclic 2-groups in Blackburn's classification are easily seen to have exponent at most 4. Consequently, a routine argument by contradiction leads to the fact that, if $\Omega_2(G)$ is metacyclic then G is itself metacyclic, assuming of course that G is 2-group. Also, notice that the four types of minimal non-metacyclic 2-groups are generated by their rational elements, as it is not difficult to check. Then we have the following result, which will prove to be very useful for our purposes.

Theorem 4.12. *Let G be a 2-group and suppose that the subgroup generated by the rational elements of G is metacyclic. Then G is metacyclic.*

In fact, by the arguments above, we can replace "rational elements" by "rational elements of order at most 4" in the statement above and the result is still true.

Let us digress from our main objective to give another characterization of the 2-groups of maximal class which is a consequence of the previous results. It follows from the proof of Theorem 4.11 above, that the subgroup generated by the rational elements in a non-abelian metacyclic 2-group which is not of maximal class is isomorphic to one of the groups $C_2 \times C_2$, $C_2 \times C_4$ or $C_2 \times C_8$. Combining these with Theorem 4.12 we get the following consequence:

Corollary 4.13. *Let G be a non-trivial 2-group and suppose that the subgroup T generated by its rational elements is metacyclic. Then either G is of maximal class (and $G = T$) or T is isomorphic to one of the subgroups C_2, $C_2 \times C_2$, $C_2 \times C_4$ or $C_2 \times C_8$.*

Hence, the 2-groups of maximal class are precisely the 2-groups whose rational elements generate a non-abelian metacyclic subgroup.

4.3 Main Results

Finally, we work to prove that 2-groups with 4 or 5 conjugacy classes of rational elements are metacyclic; as explained before, this leads to a characterization of these families of groups, by Theorem 4.11. In particular, we obtain that the 2-groups of maximal class are precisely the 2-groups which have 5 rational conjugacy classes, which is the main result in the present chapter.

4.3.1 2-Groups with 4 rational conjugacy classes

We note that the arguments used to prove that a 2-group with 4 rational classes is metacyclic are not very different to the ones needed for the 5 rational classes case. However, the proof here is shorter and somehow less involved.

Theorem 4.14. *A 2-group with 4 rational conjugacy classes is metacyclic, so the groups in the families 1 and 2 of Proposition 4.10 are all the 2-groups with 4 rational classes.*

Proof. Let G be a 2-group with 4 rational classes. If the center of G is not cyclic, then its rank must be 2, because every central involution constitutes a rational conjugacy class of G, and abelian 2-groups of rank bigger that 2 have more that 3 involutions. In this case the rational elements of G are those in $\Omega_1(\mathbf{Z}(G))$. Since this group is metacyclic, the result follows from Theorem 4.12 when $\mathbf{Z}(G)$ is not cyclic.

Now suppose that $\mathbf{Z}(G)$ is cyclic, and let z be the unique central involution of G. Of course, there are more involutions, because otherwise G is cyclic or generalized quaternion and we know that these groups have 2 or 5 rational classes. We claim that there are also rational elements of order 4. If this is not the case, the involutions (together with the trivial element) would account for all the rational, as well as the real, elements of G; in particular, by Brauer's Theorem 1.12, G would have 4 real irreducible characters. This implies that $G/\Phi(G) \cong C_2 \times C_2$ and so the 4 real irreducible characters of G would be actually rational. But the 2-groups with 4 rational irreducible characters are metacyclic, by Theorem 4.8.

So we can assume that G possesses two classes of involutions and a unique rational class containing elements of order 4. By Theorem 4.6 and Theorem 4.7, we have that

the number of involutions of G is congruent to 3 modulo 4, because cyclic 2-groups and maximal class 2-groups do not have four rational classes. Thus we have that the class of the non-central involutions has size 2. Note that if z is the unique central involution and u is a non-central involution, then uz is an involution. In particular, it is clear that the subgroup generated by all the involutions is a non-central normal subgroup isomorphic to $C_2 \times C_2$. This subgroup is not self-centralizing, since otherwise $|G| \leq 8$, so it is contained in a normal subgroup K isomorphic to $C_2 \times C_4$. Now, by Lemma 4.3, K contains rational elements of order 4, and we have that K is the subgroup generated by all rational elements of G. Since K is metacyclic, the result follows from Theorem 4.12. ∎

4.3.2 2-Groups with 5 rational conjugacy classes

We can now give a proof of the main result in this chapter, Theorem C. In this proof we have made use of the GAP software [8] at different points.

Theorem 4.15. *Let G be a 2-group with 5 conjugacy classes of rational elements. Then G is dihedral, semidihedral or generalized quaternion.*

Proof. By Theorem 4.11, it suffices to show that a 2-group with 5 rational conjugacy classes is metacydic. We argue by contradiction, assuming that G is a non-metacyclic 2-group with exactly 5 rational classes. We shall get a contradiction in a number of steps.

There is no harm in assuming that $|G| > 64$, since the result is true for 2-groups of order at most 64. This can be easily checked for instance with GAP.

Step 1. *G has rational elements of order 4.*

Suppose the contrary, working by contradiction. Then the rational elements of G are the elements of order at most 2 and they are also the real elements of G. Therefore, G has precisely 5 real conjugacy classes and 5 real irreducible characters, by Brauer's Theorem 1.12. In [20] it was proved that there are only three 2-groups with 5 real irreducible characters, which are the dihedral group of order 8, the quaternion group and the semi-dihedral group of order 16. Of course, all of them are metacyclic. (See also the comments after Theorem 4.8)

Step 2. *G has cyclic center.*

Suppose that the center of G is not cyclic. Then G has at least three central involutions and, bearing in mind Step 1, we conclude that G has no more involutions and a unique conjugacy class of rational elements of order 4. By Lemma 4.5, we conclude that if x is a rational element of order 4, then the subgroup generated by the rational elements of G is $T = \langle x \rangle N$, where $N = \Omega_1(G) \cong C_2 \times C_2$. Obviously $T \cong C_2 \times C_4$, which is metacyclic, so G is metacyclic too by Theorem 4.12, against our hypothesis.

For the rest of the proof, let z be the unique central involution of G.

Step 3. *G has 2 or 3 conjugacy classes of involutions.*

Since G has rational elements of order 4, it cannot have more than three classes of involutions. On the other hand the 2-groups with exactly one class of involutions are the 2-groups with one involution, which are metacyclic by Theorem 4.2.

Step 4. *G has a non-central normal elementary abelian subgroup N of order 4.*

By Theorem 4.6 and Theorem 4.7, G contains a conjugacy class of involutions of size 2, which for the rest of this proof, will be supposed to be that of the element u. By the previous step, there is at most another conjugacy class of involutions and, if it exists, its size will have to be a multiple of 4, so the class of u is the unique class of involutions of size 2 and, since this is also the size of the class of uz, we conclude that the class of u consists precisely of u and uz. Then $N = \langle u, z \rangle$ is a non-central normal subgroup of G isomorphic to $C_2 \times C_2$.

Step 5. *G has no normal elementary abelian subgroup of order 8.*

We suppose that G possesses a normal elementary abelian group L of order 8. Then G has three classes of involutions, all of them contained in L, so $L = \Omega_1(G)$. Now, $\mathrm{Aut}(L) \cong \mathrm{GL}(3,2)$, the group of invertible matrices of size 3×3 with entries in the field of size 2. This group has a Sylow 2-subgroup of order 8, so L does not self-centralize, as $|G| > 8\,|L| = 64$. Therefore there exists an abelian normal subgroup T containing L with $|T : L| = 2$ and necessarily $T \cong C_2 \times C_2 \times C_4$.

We claim that $|\mathbf{C}_T(g)| \geq 4$ for any $g \in G$. This is clear if $|\mathbf{C}_L(g)| \geq 4$, so we can assume that $\mathbf{C}_L(g) = \langle z \rangle$. Then there exists $v \in L - N$ such that $v^g = vu$ and $u^g = uz$. Now let $n = o(g)$ and notice that $g^{n/2} \in L$, so $g^{n/2} = z$. The action of g on L has order 4, so $n \geq 8$. Moreover, if $n = 8$, then $g^4 = z$ and vg^2 is an involution not lying in L, a contradiction. Finally, if $n \geq 16$, $g^{n/4}$ acts trivially on T (this is because for any $x \in T \setminus L$, $x^g = xw$ for some $w \in L$ and $x^{g^4} = xww^gw^{g^2}w^{g^3} = x$) so, if we take an element $x \in T \setminus L$, $x^2 = z$ and $xg^{n/4}$ is an involution. Therefore $g^{n/4} \in T$ and $|\mathbf{C}_T(g)| \geq 4$, as desired.

Next we see that there exist elements $g \in G$ with $|\mathbf{C}_L(g)| = 2$. Indeed, the factor group $G/\mathbf{C}_G(L)$ is naturally isomorphic to a subgroup H of the group of unipotent automorphisms of L (those stabilizing the chain $\langle z \rangle < N < L$), which is isomorphic to D_8. There are two maximal subgroups of D_8 of exponent 2: one corresponds to the group of automorphisms of L that fix N elementwise, and the other to the group of automorphsims that induce the identity on $L/\langle z \rangle$. The actions of these two groups on L have 5 orbits, so we conclude that $G/\mathbf{C}_G(L)$ must have exponent 4, which means that there exists an element $g \in G$ such that $v^g = vu$, $u^g = uz$ and this is the element desired.

If g is as in the last paragraph, then $\mathbf{C}_T(g)$ is not contained in L, so there exists an element $x \in T \setminus L$ that commutes with g. Notice that $T^2 = \langle z \rangle$, so $x^2 = z$ and $(xu)^g = (xu)^{-1}$. Therefore T is the subgroup generated by the rational elements of G. In fact, by conjugating by g and g^2, one can check that all the elements xw for $w \in L$, $w \neq 1, z$ are rational, so the conjugacy class of x contains these six elements and it must be the full set of elements of order 4 in T.

Let H be now the subgroup of $\mathrm{Aut}(T)$ defined by the action of G on T. Then the orbit of x under H is the conjugacy class of x, which has size 8, and the stabilizer of x in H contains the automorphism induced by g, which has order 4, so we conclude that $|H| \geq 32$. In fact, H is contained in the group P of automorphisms of T that act unipotently on L. The group P has order 64 and $H \neq P$ because there are elements $\sigma \in P$ such that $|\mathbf{C}_T(\sigma)| = 2$, so H is a maximal subgroup of P.

It can be checked, either by hand or with the help of GAP, that of the 7 maximal subgroups of P only one satisfies the conditions that its action on L has 4 orbits, the

elements of order 4 in T form a unique orbit and every element acts on T fixing at least four elements. It turns out that this unique maximal subgroup contains the automorphisms α and β defined by $x^\alpha = xu$, $v^\alpha = vz$, $u^\alpha = u$, $z^\alpha = z$ and $x^\beta = xv$, $v^\beta = v$, $u^\beta = uz$, $z^\beta = z$. Then let $K \leq G$ be the subgroup corresponding to $\langle \alpha, \beta \rangle \cong C_2 \times C_2$ under the map $G \to H$ given by conjugation of G on T. As one can immediately see, K has 5 classes of elements of order at most 2 but no rational elements of order 4 and, containing L, is not metacyclic. This contradicts Step 1 and this contradiction proves this step.

Step 6. *G has a normal subgroup K isomorphic to $C_2 \times C_4$ that contains elements rational in G of order 4, and a subgroup $T \cong C_2 \times C_2 \times C_4$ with $K \subseteq T$.*

It is clear that N is not a maximal normal abelian subgroup of G, so there exists a normal abelian subgroup K with $|K : N| = 2$. Since G has no normal elementary abelian subgroups of order 8, $K \cong C_2 \times C_4$. Then, from Lemma 4.3, K contains some element x of order 4 which is rational in G. In addition, $K^2 = \langle x^2 \rangle$ is a cyclic normal subgroup of order 2, so $x^2 = z$ and $K = \langle u, x \rangle$.

Let H be the image of the natural homomorphism from G to $\mathrm{Aut}(K) \cong D_8$ induced by conjugation and notice that there must be elements in H (possibly distinct) sending u to uz and x to x^{-1}. If H has exponent 2 the only possibility is that H is generated by the inversion map and the automorphism $u \mapsto uz$, $x \mapsto x$. But then the 5 rational classes of G are those of the elements 1, z, u, x and xu, so the rational elements of G generate K, which is metacyclic and G would be metacyclic too, by Theorem 4.12. We conclude that H has exponent 4 and so there exists an element $g \in G$ such that $x^g = xu$ and $u^g = uz$. Thus the 4 elements of order 4 in K form a rational conjugacy class in G.

Since $|G| > 64$, K is not self-centralizing, and so there exists an abelian normal subgroup R containing K with $|R : K| = 2$. If $R \cong C_2 \times C_2 \times C_4$, we are done. So we can assume that $R \cong C_2 \times C_8$ or $R \cong C_4 \times C_4$. In the former case R^2 is a cyclic normal subgroup of order 4 contained in K, but K has no such subgroup (recall that all the elements of order 4 in K are conjugate), so $R \cong C_4 \times C_4$ and we can write $R = \langle t, x \rangle$ with $t^2 = u$.

Now let $n = o(g)$. If $n \geq 8$, then $g^{n/2}$ is an involution that centralizes K, so if this element is not in K, we simply take $T = K\langle g^{n/2} \rangle$. Thus we suppose that $g^{n/2} \in K$, which actually means that $g^{n/2} = z$.

If $n \geq 16$, then $g^{n/4}$ commutes with x and $(xg^{n/4})^2 = 1$. Moreover, $xg^{n/4} \notin K$, so $T = K\langle xg^{n/4} \rangle$ is the desired subgroup.

We finally argue that, when $n = 4$ or $n = 8$, G has more than 5 rational classes. We have to consider how the action of $\langle g \rangle$ on K moves t. Of course $t^g = txw$ for some $w \in N$ and we can suppose that $w = 1$ or $w = u$. In any case $\mathbf{C}_R(g) = \langle z \rangle$.

If $n = 8$, then $\langle x, g^2 \rangle \cong Q_8$, so g^2 is a rational element of order 4 not contained in R. Now, if $w = 1$, then $g^2 t$ is an involution outside N, so we would have at least 6 rational conjugacy classes. On the other hand, if $w = u$, then $t^{g^2} = t^{-1}$ and again we have at least 6 rational classes.

The remaining case is when $n = 4$. Then $R \cap \langle g \rangle = 1$ and g^2 is an involution outside N. If $w = 1$, then $g^2 t$ has order 4 and is inverted by x, whereas, if $w = u$, $t^{g^2} = t^{-1}$. In any case there are at least 6 rational classes.

Step 7. *The final contradiction.*

Let v be an involution not conjugate to z or u. By the previous step we can suppose that v centralizes K. We claim that $L = \Omega_1(G)$ is non-abelian for, otherwise, it is elementary abelian and therefore the union of N and the class of v, whence $|L| = 4 + |\mathrm{Cl}_G(v)|$. Since $|L|$ and $|\mathrm{Cl}_G(v)|$ are powers of 2 the only possibility is that $|\mathrm{Cl}_G(v)| = 4$ and $|L| = 8$, so that L is indeed elementary abelian of order 8, against Step 5.

So v does not commute with some of its conjugates, say v'. Then v and v' generate a dihedral group and vv' is inverted by v. Therefore a power of vv' is an element of order 4 inverted by v and contained in K, which contradicts the fact that v centralizes K. This is the final contradiction.

Chapter 5

Quadratic rational solvable groups

5.1 Introduction

The study of fields of values is a relevant topic in representation theory of finite groups, and in this context problems on rationality are probably among the most interesting ones. Indeed, it is quite a natural question to ask how fields generated by values of characters reflect, and are reflected in the structure of a finite group. Several results in the literature are devoted to rational groups, i. e. groups all whose characters are rational valued, and more generally to groups with small fields of values. A frequent approach to these type of questions consists in analyzing the composition factors of a group in the family under consideration.

To a certain extent, for a solvable group G classifying the composition factors of the group amounts to determining the prime divisors of the order of G. In his well-known work [9], R. Gow proved that a rational solvable group has order only divisible by the primes 2, 3 and 5. In a similar fashion, E. Farias e Soares provided a more general, independent bound for the set of primes dividing the order of a group G, in terms of the degree of the field of values of the group over $\mathbb{Q}$, where G is any finite solvable group [6].

It is interesting to note that the bound given by Farias e Soares cannot be significantly improved, in the sense that it is polynomial of degree two, and no linear bound of the same type does exist. However, it appears that R. Gow's result cannot be recovered from [6].

More recent work by D. Chillag and S. Dolfi [3] treats solvable groups satisfying the condition that all its elements are either rational or quadratic. As these authors show, the order of a group in this family is divisible only by primes in the set $\{2, 3, 5, 7, 13, 17\}$, although no example for the prime 17 is available. One of the main results in this chapter deals with the dual situation for characters. We recall that a character χ of G is quadratic if $|\mathbb{Q}(\chi) : \mathbb{Q}| = 2$, and we say that a group G is **quadratic rational** if every $\chi \in \mathrm{Irr}(G)$ is either rational or quadratic.

Theorem D. *Let G be a quadratic rational solvable group, and p a prime divisor of $|G|$. Then p lies in $\{2, 3, 5, 7, 13\}$.*

Note that if p lies in $\{2, 3, 5, 7, 13\}$, then the Frobenius group of order $p(p-1)/2$ is quadratic rational, so Theorem D is sharp.

Some comments about the non-solvable case are perhaps appropriate. In this more general setting, W. Feit and G. Seitz described the non-abelian composition factors of a rational group [7], and J. Thompson [36] proved that the primes that can occur as the order of a cyclic composition factor of a rational group are smaller or equal to 11. As an indication of the difficult nature of these problems, it still continues to be an open question to show that 7 and 11 cannot occur as the order of an abelian composition factor of a rational group.

If we drop the solvability assumption in Theorem D above, it seems that the possible non-abelian composition factors that may occur in a quadratic rational group can be determined, and this problem is treated in work in preparation by P. H. Tiep. Naturally, it remains a challenge to classify the primes dividing the cyclic composition factors of quadratic rational groups.

In this chapter, we shall also show that Theorem D can be generalized, in order to obtain a bound for the set of primes dividing the order of a solvable group whose irreducible characters have small field of values, answering a question of A. Moretó.

Theorem E. *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that for any solvable group G and any prime divisor p of $|G|$, if $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ for all $\chi \in \mathrm{Irr}(G)$ then $p \leq f(k)$.*

The **field of values** of a finite group G is defined as the smallest field containing all character values of the group:

$$\mathbb{Q}(G) = \{\chi(g) \,|\, g \in G,\ \chi \in \mathrm{Irr}(G)\}\,.$$

As a consequence of Theorem E, there exists a function $d : \mathbb{N} \to \mathbb{N}$ such that for any solvable group G and any prime divisor p of $|G|$, if $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ for all $\chi \in \mathrm{Irr}(G)$ then $|\mathbb{Q}(G) : \mathbb{Q}| \leq d(k)$, as will become clear later (see Section 5.4 below). We note that Theorem E can be viewed as a stronger form of the main result in the work by Farias e Soares [6], as the main theorem in [6] states that for G solvable, the set of primes dividing $|G|$ is bounded by a function of $|\mathbb{Q}(G) : \mathbb{Q}|$.

The chapter is organized as follows. We start with some preliminary results in Section 5.2, and proofs of the main results are given in Section 5.3. An interesting question posed by Chillag and Dolfi in [3] is answered in Section 5.4. Finally, Section 5.5 is devoted to some examples and remarks.

The main results in this chapter have been obtained by the author and appear in [35].

5.2 Preliminary Results

In this section we present the results needed for the proofs of Theorem D and Theorem E.

Following the nomenclature in [3], an element $x \in G$ is called **semi-rational** in G if there exists an integer m such that any generator of $\langle x \rangle$ is conjugate in G to either x or x^m. Also, a group G is **semi-rational** if all its elements are semi-rational. The main result in [3] states that if p is a prime divisor of a semi-rational solvable group, then p lies in $\{2, 3, 5, 7, 13, 17\}$, and examples are provided of semi-rational solvable groups of order divisible by the primes in the list, except for 17.

Theorem 5.1. *Let G be a semi-rational solvable group and p a prime divisor of $|G|$. Then p lies in $\{2,3,5,7,13,17\}$.*

Proof. See Theorem B of [3]. ▮

Let us start by proving the following easy characterization of semi-rational elements in terms of their fields of values. Recall that an element x of a group G is quadratic if $|\mathbb{Q}(x):\mathbb{Q}| = 2$.

Lemma 5.2. *Let $x \in G$. Then x is semi-rational in G if and only if x is either rational or quadratic in G.*

Proof. Let $n = o(x)$ and $\xi \in \mathbb{C}$ a primitive nth root of unity. By 1.3, the map

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) & \longrightarrow & \mathrm{Aut}(\langle x\rangle) \\ \sigma & \mapsto & f \end{array} \tag{5.1}$$

defined by $f(x) = x^t$ when $\xi^\sigma = \xi^t$, where $1 \le t \le n$ is an integer coprime to n, is a well-defined group isomorphism. We can identify $\mathbf{N}_G(\langle x\rangle)/\mathbf{C}_G(x)$ with a subgroup of $\mathrm{Aut}(\langle x\rangle)$ in the obvious way, as in 2.4. Then, by the comments before 2.6, the isomorphism 5.1 restricts to a group isomorphism

$$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(x)) \longrightarrow \mathbf{N}_G(\langle x\rangle)/\mathbf{C}_G(x).$$

The result now follows, as it is easy to check that x is semi-rational in G if and only if $\mathbf{N}_G(\langle x\rangle)/\mathbf{C}_G(x)$ has index at most 2 in $\mathrm{Aut}(\langle x\rangle)$, and x is quadratic in G if and only if $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(x))$ has index at most 2 in $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$, by basic Galois theory. ▮

We recall that if $M \lhd G$, $\theta \in \mathrm{Irr}(M)$ and T, T^* are the inertia and semi-inertia groups of θ in G, respectively, then by 2.1 there exists a natural isomorphism

$$\rho_\theta = \rho : \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G)) \longrightarrow T^*/T, \tag{5.2}$$

where $\rho(\sigma)$ is the unique (modulo T) element in T^* such that

$$\theta^\sigma = \theta^{\rho(\sigma)},$$

for any $\sigma \in \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G))$.

Lemma 5.3. *Let G be a finite group satisfying that $|\mathbb{Q}(\chi):\mathbb{Q}| \le k$ for all $\chi \in \mathrm{Irr}(G)$. Supose that $M \lhd G$ with $(|M|, |G/M|) = 1$, and let $\theta \in \mathrm{Irr}(M)$. Then $\rho^{-1}(T^*/T)$ is a subgroup of index at most k of $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$, where T and T^* are the inertia and semi-inertia groups of θ in G, respectively, and ρ is defined as in 5.2.*

Proof. The map

$$\varphi : T^* \longrightarrow \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G))$$

defined by $g \mapsto \sigma$, whenever $\theta^g = \theta^\sigma$, is a well-defined, surjective group homomorphism with kernel T, by Lemma 2.4. Let $\hat{\theta} \in \mathrm{Irr}(T)$ be the canonical extension of θ, and recall that $\mathbb{Q}(\hat{\theta}) = \mathbb{Q}(\theta)$. By Clifford's correspondence, we have that $\psi = \hat{\theta}^G \in \mathrm{Irr}(G)$. So by hypothesis $|\mathbb{Q}(\psi) : \mathbb{Q}| \leq k$.

Now, we claim that $\mathbb{Q}(\theta^G) = \mathbb{Q}(\psi)$. Of course, the Galois group $\mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ acts naturally on the sets of characters of G and M. Now, by elementary Galois theory it suffices to show that the characters θ^G and ψ are fixed precisely by the same field automorphisms of $\mathbb{Q}_{|G|}$.

Suppose first that $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ is such that $\psi^\sigma = \psi$. Since $M \lhd G$, we have that $\theta^\sigma = \theta^g$ for some $g \in G$, by Clifford correspondece. Then $(\theta^G)^\sigma = (\theta^\sigma)^G = (\theta^g)^G = \theta^G$.

Assume now that $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ fixes θ^G. By Theorem 1.7 we have that $\theta^\sigma = \theta^g$ for some $g \in T^*$, so $\theta = (\theta^g)^{\sigma^{-1}}$. In particular g normalizes T and, if $\hat{\theta}$ is the canonical extension of θ to T, then $(\hat{\theta}^g)^{\sigma^{-1}} = \hat{\theta}$ by uniqueness of the canonical extension. So $\hat{\theta}^\sigma = \hat{\theta}^g$ and thus

$$(\hat{\theta}^G)^\sigma = (\hat{\theta}^\sigma)^G = (\hat{\theta}^g)^G = \hat{\theta}^G.$$

Finally, the claim implies that φ is a bijection from T^*/T onto $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\psi))$, and by Galois theory we have that $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\psi))$ is a subgroup of index at most k in $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$. ∎

We remark that in the notation of Lemma 5.3, we have that if G is quadratic rational then T^*/T is isomorphic to a subgroup of index a divisor of 2 of $\mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$, for every $\theta \in \mathrm{Irr}(M)$.

5.2.1 Fields of Values and Brauer Characters

We shall need a result on fields of values of Brauer characters, which we present next. However, some preparation is required in order to prove it: first, we recall the definition and some basic facts of Brauer characters, and later we give account of some results on splitting fields of groups. For a detailed exposition on the theory of Brauer characters, we refer to G. Navarro's book [27], and a development of the elementary theory of splitting fields can be found on Chapter 9 of [13] by M. Isaacs.

Let R be the ring of algebraic integers in $\mathbb{C}$, and fix a prime p. We choose a maximal ideal I of R containing the ideal pR (of the multiples of p in R) and we write

$$F = R/I\,. \tag{5.3}$$

Since I is a maximal ideal, we have that F is a field, and it is immediate to see that the characteristic of F is p. Let

$$^* : R \longrightarrow F$$

be the canonical homomorphism. Also, write

$$U = \{\xi \in \mathbb{C} \mid \xi^m = 1 \text{ for some integer } m \text{ not divisible by } p\} \subseteq R,$$

for the multiplicative group of complex p'th roots of unity. If we write $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, then we have the following.

Lemma 5.4. *The restriction of * to U defines an isomorphism $U \to F^\times$ of multiplicative groups, and F is the algebraic closure of its prime field $\mathbb{Z}^* \cong \mathbb{Z}_p$.*

Proof. This is Lemma 2.1 of [27]. ▮

Suppose now that $\mathcal{X} : G \to \mathrm{GL}(n, F)$ is a representation of G, and let g be a p-regular element of G, that is an element of order not divisible by p. Observe that all eigenvalues of $\mathcal{X}(g)$ lie in $F^\times$, since $\mathcal{X}(g)$ is an invertible matrix and F is algebraically closed, by Lemma 5.4. Then, we have that all the eigenvalues of $\mathcal{X}(g)$ are of the form $\xi_1^*, \ldots, \xi_n^*$ for uniquely determined $\xi_1, \ldots, \xi_n \in U$, again by Lemma 5.4. The complex map φ defined on the set of p-regular elements of G by

$$\varphi(g) = \xi_1 + \cdots + \xi_n,$$

for any p-regular element g of G, is the **Brauer character** of G afforded by the representation $\mathcal{X}$. The characteristic of the field F is sometimes made explicit by saying that φ is a p-Brauer character of G. Notice that φ is uniquely determined by the equivalence class of the representation $\mathcal{X}$ (once the ideal I has been chosen) and φ is constant on conjugacy classes of p-regular elements. Also, it is possible to prove that if φ is a Brauer character of G and

$$\varphi(g) = \xi_1 + \cdots + \xi_n,$$

where $g \in G$ is p-regular and the $\xi_i \in U$ are uniquely determined as above, then $o(\xi_i)$ divides $o(g)$ for all i (this follows from the comments on page 18 of [27], for instance).

A Brauer character of G is **irreducible** if it is afforded by an irreducible F-representation of G, and the set of irreducible Brauer characters of G is usually denoted by $\mathrm{IBr}(G)$.

Theorem 5.5. *The set $\mathrm{IBr}(G)$ is a basis for the complex functions which are constant on the conjugacy classes of p-regular elements of G.*

Proof. See Lemma 2.10 of [27]. ▮

It follows from the last theorem, that a Brauer character φ of G can be uniquely expressed as a non-negative integer linear combination of irreducible Brauer characters of G. The characters appearing in such a decomposition are called the **irreducible constituents** of φ. Recall also that only when the characteristic p of F divides $|G|$, the theory of Brauer characters has special interest.

Theorem 5.6. *If p does not divide $|G|$, then $\mathrm{IBr}(G) = \mathrm{Irr}(G)$.*

Proof. This is Lemma 2.12 of [27]. ∎

Let φ is a p-Brauer character of G. Then the **field of values** of φ is defined in the obvious way

$$\mathbb{Q}(\varphi) = \mathbb{Q}(\varphi(g) \mid g \in G \text{ is } p\text{-regular}).$$

By the comments after the definition of Brauer character, it is clear that $\mathbb{Q}(\varphi) \subseteq \mathbb{Q}_{|G|_{p'}}$. Suppose that $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$. Then φ^σ is the complex map defined on the set of p-regular elements of G by

$$\varphi^\sigma(g) = \varphi(g)^\sigma,$$

for every p-regular $g \in G$. It is not true in general that for $\varphi \in \mathrm{IBr}(G)$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$, the map φ^σ is an irreducible Brauer character of G (see [27], page 43).

We need some more notation. Let $K \subseteq L$ be a field extension, and let $\mathcal{Y}$ be a K-representation of the group G. Then $\mathcal{Y}(g)$ is an invertible matrix with entries in K, for any $g \in G$, and it is clear that $\mathcal{Y}(g)$ is also invertible in L. Therefore, we can view $\mathcal{Y}$ as an L-representation of G, and as such we denote it by $\mathcal{Y}^L$, following the notation in [13], Chapter 9.

As is well-known, Brauer characters arise in solvable groups in a natural way. If G is solvable and M is a minimal normal subgroup of G, then M is an elementary abelian p-group, for some prime p. In particular, we have that $V = \mathrm{Irr}(M)$ is a vector space over the field of p elements $\mathbb{Z}_p$, with the product of characters of M as addition of vectors. More precisely, if $\mu \in \mathbb{Z}_p$ and t is an integer with $t + p\mathbb{Z} = \mu$, then we write

$$\mu\theta = \theta^t,$$

and this product does not depend on the choice of t. Observe that V has the structure of a $\mathbb{Z}_p[G]$-module, with the action of G on V by conjugation, and V is irreducible because M is minimal normal. In general, if v is a vector of a module V of G and $g \in G$, then $v^g = vg$ denotes the image of v under the map induced by g on V.

Using the same notation, suppose that $\mathcal{X}$ is an irreducible $\mathbb{Z}_p$-representation of G afforded by M. Since the prime field of F is isomorphic to $\mathbb{Z}_p$, we can view $\mathcal{X}$ as an F-representation of G, and as such we denote it by $\mathcal{X}^F$, by a slight abuse of notation. Observe that the representation $\mathcal{X}^F$ affords a Brauer character of G which is not necessarily irreducible. We are interested in the field of values of Bauer characters arisen in this way, when G is quadratic rational.

As we said before, we need some basic facts on splitting fields of groups. Suppose that $\mathcal{Y}$ is a K-representation of G, where K is an arbitrary field. Then $\mathcal{Y}$ is **absolutely irreducible** if $\mathcal{Y}^L$ is irreducible for every field $L \supseteq K$. Also, a field K is a **splitting field** of G if every irreducible K-representation of G is absolutely irreducible.

Theorem 5.7. *If K is an algebraically closed field, then K is a splitting field for any group.*

Proof. This is Corollary 9.4 of [13]. ▮

The following result is true for any field, but we do not need it in all its generality.

Theorem 5.8. *Suppose that K is a splitting field of G. Then there are finitely many similarity classes of irreducible K-representations of G. Also, the characters of non-similar irreducible K-representations of G are are nonzero, distinct, and linearly independent over K.*

Proof. See Corollary 9.4 and Lemma 9.12 of [13]. ▮

We denote the set of characters afforded by irreducible K-representations of G by $\mathrm{Irr}(G)_K$. Next we indicate how to define Galois action on the set $\mathrm{Irr}(G)_K$.

Suppose that $T \subseteq K$ is a field extension, where K is a splitting field of G. Let $\chi \in \mathrm{Irr}(G)_K$, and write

$$T(\chi) = T(\chi(g) \mid g \in G)$$

for the smallest subfield of K containing T and all the values of χ. It is not difficult to prove that $T(\chi)$ is a finite degree Galois extension over T and the expression

$$\chi^\tau(g) = \chi(g)^\tau,$$

where $g \in G$ and $\tau \in \mathrm{Gal}(T(\chi)/T)$, defines a regular action of $\mathrm{Gal}(T(\chi)/T)$ on the set

$$\{\psi \in \mathrm{Irr}(G)_K \mid T(\psi) = T(\chi)\}.$$

A pair of characters $\chi, \psi \in \mathrm{Irr}(G)_K$ are called Galois conjugate over T, whenever $T(\chi) = T(\psi)$ and there exist $\tau \in \mathrm{Gal}(T(\chi)/T)$ such that $\psi = \chi^\tau$.

Theorem 5.9. *Suppose that $T \subseteq K$, where K is a splitting field of G, and assume that $\mathrm{char}(T) \neq 0$. Also, let $\mathcal{Y}$ be an irreducible T-representation of G. Then all irreducible constituents of $\mathcal{Y}^K$ occur with multiplicity one, and the characters that these constituents afford are Galois conjugate over T.*

Proof. See Theorem 9.21 of [13]. ▮

We are now able to give a proof of the announced result on fields of values of Brauer characters. Suppose that $\mathcal{X}$ is an irreducible $\mathbb{Z}_p$-representation of the finite group G. Arguing as before, we can view $\mathcal{X}$ as an F-representation of G, and we denote it by $\mathcal{X}^F$, where F is the field defined in 5.3. Now, every irreducible constituent of $\mathcal{X}^F$ affords an irreducible Brauer character of G, and it is clear that these Brauer characters are the irreducible constituents (counting multiplicities) of the Brauer character of G afforded by $\mathcal{X}^F$.

Theorem 5.10. *Let G be a finite group and $\mathcal{X}$ an irreducible $\mathbb{Z}_p$-representation of G. If $\psi, \varphi \in \mathrm{IBr}(G)$ are irreducible constituents of the Brauer character of G afforded by $\mathcal{X}^F$, then $\psi^\sigma = \varphi$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$.*

Proof. Recall that by Theorem 5.4 the field F is algebraically closed, and thus F is a splitting field for G, by Theorem 5.7. Then all irreducible constituents of $\mathcal{X}^F$ occur with multiplicity one, by Theorem 5.9; furthermore, the F-characters of G afforded by these representations are Galois conjugate over the field $E = \mathbb{Z}_p$, by the same result.

Suppose now that $\mathcal{Y}, \mathcal{Z}$ are two irreducible constituents of $\mathcal{X}^F$, and assume that they afford the Brauer characters ψ and φ of G, respectively. Also, let ν, δ be F-characters of G afforded by $\mathcal{Y}$ and $\mathcal{Z}$, respectively. Then we have that ν and δ are Galois conjugate over E, i. e.

$$E(\nu) = E(\delta) = L$$

and there exists $\alpha \in \mathrm{Gal}(L/E)$ such that $\nu^\alpha = \delta$. Note that the field F is an algebraic closure of L, so by uniqueness of algebraic clousures there exists a field automorphism $\rho : F \to F$ extending α.

Now we consider the group automorphism $\tau \in \mathrm{Aut}(U)$ obtained by first composing $^* : U \to F^\times$, then the restriction $\rho_{F^\times} : F^\times \to F^\times$, and afterwards the inverse of $^* : U \to F^\times$. It is clear that τ permutes the set of primitive $|G|_{p'}$th roots of unity. Then, if $\xi \in U$ a fixed $|G|_{p'}$th-root of unity, we have that $\tau(\xi) = \xi^m$ for an integer m coprime with $|G|_{p'}$. By Galois theory, there exists a unique $\sigma \in \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q}_{|G|_p})$ such that $\sigma(\xi) = \xi^m$, and it is clear that $\sigma(\lambda) = \lambda^m$ for all $\lambda \in \langle\xi\rangle$.

Observe that if we apply the field automorphism ρ to every entry of the matrix $\mathcal{Y}(g)$, for every $g \in G$, we obtain a new representation of G, which we denote by $\mathcal{Y}^\rho$. It is easy to see that $\mathcal{Y}^\rho$ is irreducible, and of course $\mathcal{Y}^\rho$ affords the F-character δ of G. Then, by Theorem 5.9, $\mathcal{Y}^\rho$ is similar to $\mathcal{Z}$. In particular, $\mathcal{Y}^\rho$ affords the Brauer character φ of G. Hence, in order to prove the result it suffices to show that the Brauer character of G afforded by $\mathcal{Y}^\rho$ is ψ^σ.

Let g be a p-regular element of G. It is not difficult to check that if $\epsilon_1, \ldots, \epsilon_n$ are the eigenvalues of $\mathcal{Y}(g)$ in F, then $\rho(\epsilon_1), \ldots, \rho(\epsilon_n)$ are the eigenvalues of $\mathcal{Y}^\rho(g)$ in F. Now, if $\lambda_1, \ldots, \lambda_n \in U$ are such that $(\lambda_i)^* = \epsilon_i$, then $\psi(g) = \lambda_1 + \cdots + \lambda_n$. Note that $o(g)$ divides $|G|_{p'}$, and recall that $o(\lambda_i) = o(\epsilon_i)$ divides $o(g)$, so $\lambda_i \in \langle\xi\rangle$. Hence $(\lambda_i{}^m)^* = \rho(\epsilon_i)$. Therefore, if η is the Brauer character of G afforded by $\mathcal{Y}^\rho$, then

$$\eta(g) = \lambda_1{}^m + \cdots + \lambda_n{}^m = \psi(g)^\sigma = \psi^\sigma(g)\,,$$

and the result follows. ∎

Notice that, in the notation of Theorem 5.10, it is clear that $\mathbb{Q}(\psi)^\sigma = \mathbb{Q}(\varphi)$, by definition of the field of values of ψ. Of course, $\mathbb{Q}_{|G|}/\mathbb{Q}$ is an abelian, Galois extension, and thus by basic Galois theory we have that $\mathbb{Q}(\psi)/\mathbb{Q}$ is a normal extension. Then, we deduce that $\mathbb{Q}(\psi) = \mathbb{Q}(\varphi)$. In particular, the values of the Brauer character of G afforded by $\mathcal{X}^F$ are contained in $\mathbb{Q}(\varphi)$, for any irreducible constituent $\varphi \in \mathrm{IBr}(G)$ of the Brauer character afforded by $\mathcal{X}^F$. We shall use this consequence of Theorem 5.10 in the proof of Theorem D and Theorem E.

5.2.2 Farias e Soares theorem

The last ingredient that we need to prove the main theorems in this chapter is a result that essentially contains the conclusions of the work by Farias e Soares [6]. We start with

a definition that already appeared in Gow's paper [9].

Suppose that G acts on a finite-dimensional vector space V over a finite field F. The action of G on V is said to have the h-**eigenvalue property**, for a positive integer h, provided that h divides $|F^\times|$, and that for every v in V, there exists $g \in G$, such that $v^g = \mu v$ where μ is some fixed element of order h in $F^\times$, the group of units of F.

Note that since $F^\times$ is a cyclic multiplicative group, the choice of the particular element μ of order h in the previous definition is not relevant. Also, if the action of G on V has the h-eigenvalue property, it is immediate that it also has the l-eigenvalue property for every divisor l of h.

The following result, which is contained in Theorem B of [6], is essential in our proofs of Theorem D and Theorem E.

Theorem 5.11 (Farias e Soares). *Let a solvable group G act on a finite dimensional $\mathbb{Z}_p$-vector space V, with the prime p not dividing $|G|$. If the action has the h-eigenvalue property and η is the Brauer character afforded by V, then either $|\mathbb{Q}(\eta) : \mathbb{Q}| \geq p/(6\sqrt{3})$ or $\mathbb{Q}(\eta)$ contains a primitive $(h/(h,4))$th root of unity. In any case, if $q \neq 3$ is a prime divisor of h then $\mathbb{Q}(\eta)$ contains a primitive qth root of unity.*

Note that the character η in Theorem 5.11 is in fact an ordinary character of G; of course this follows from Theorem 5.6 because p does not divide $|G|$.

Apart from Theorem 5.11, we find it useful to apply to the following technical results from [6]. We recall that the action of a group G on another group H is said to be a **Frobenius** action, if the identity of H is the unique fixed point of any nonidentity element of G; in this case G is called a **Frobenius complement**.

Lemma 5.12. *Let G be a finite group acting on a finite dimensional $\mathbb{Z}_p$-vector space V, where the prime p does not divide $|G|$. Suppose that the action of G on V is Frobenius, and let η be the Brauer character afforded by V. Let $g \in G$ have order r. Then the value of the Euler function $\Phi(r)$ divides $|\mathbb{Q}(\eta) : \mathbb{Q}|\dim_{\mathbb{Z}_p} V$.*

Proof. See Lemma 4.3 of [6]. ∎

Suppose that G is a Frobenius complement, and let q be a prime divisor of $|G|$. Then by Corollary 6.17 of [14], a Sylow q-subgoup of G is either cyclic or generalized quaternion. Furthermore, assume that all Sylow q-subgroups of G are cyclic if $q = 2$; then, by Lemma 3.4 of [6], $\mathbf{O}^{q'}(G)$ has a normal q-complement L, and either (i) L is cyclic or (ii) $q = 3$ and $\mathbf{O}_2(G) \cong Q_8$. In any case, L has a cyclic normal 2-complement.

Another known fact about the structure of Frobenius complements that we shall use is the following. Suppose that G is a Frobenius complement and assume that $S \in \mathrm{Syl}_2(G)$ is not cyclic; then $\mathbf{O}_2(G)$ has index at most 4 in S (see Lemma 3.3 of [6]).

Lemma 5.13. *Assume the hypothesis in Lemma 5.12, for G solvable and $p > 7$. In addition, assume that $r = q^n$ with q a prime, and that the action has the r-eigenvalue property; also, if $q = 2$ suppose that the Sylow 2-subgroups of G are cyclic. Then, if $\mathbb{Q}(\eta)$ does not contain a primitive rth root of unity, we have that $\dim V = qd$ for some integer d satisfying*

$$|L| \geq \frac{p^{qd}-1}{q(p^d-1)}$$

and

$$\Phi(|L|) \geq \frac{(q-1)d(qd-d+1)}{2}$$

where L is the normal q-complement of $\mathbf{O}^{q'}(G)$. In the exceptional case where $q = 3$ and $\mathbf{O}_2(G) \cong Q_8$, then

$$|A| \geq \frac{p^{2d}+p^d+1}{12}$$

and

$$\Phi(|A|) \geq 4d^2$$

where A is the normal 2-complement of L.

Proof. See Lemma 4.12 of [6]. ▮

The reason why we introduced Frobenius action is provided by the next result; as we shall see, this lemma allows us to reduce the proof of Theorem D to a question about this type of action.

Lemma 5.14. *Let H be a finite group acting on a vector space V over the finite field $\mathbb{Z}_p$, and assume that p does not divide $|H|$. Suppose that the action has the h-eigenvalue property, and let η be the Brauer character of G afforded by V. Let M be a maximal element of*

$$\{\mathbf{C}_H(v) \mid v \in V,\ v \neq 0\}$$

with respect to inclusion, $N = \mathbf{N}_H(M)$ and $W = \mathbf{C}_V(M)$. Then the action of N/M on W is Frobenius, it has the h-eigenvalue property and, if η_0 is the Brauer character of N/M afforded by W, then $\mathbb{Q}(\eta_0) \subseteq \mathbb{Q}(\eta)$

Proof. See Lemma 4.1 of [6]. ▮

5.3 Main Results

Now we work towards a proof of Theorem D.

Theorem 5.15. *Let G be a quadratic rational solvable group and p a prime divisor of $|G|$. Then $p \leq 19$ and $p \neq 11$.*

Proof. We work by induction on $|G|$.

First, note that we can assume that G has a unique minimal normal subgroup. Otherwise, let M_1 and M_2 be two distinct minimal normal subgroups of G, so G is isomorphic to a subgroup of the direct product $G/M_1 \times G/M_2$. Observe that G/M_i is quadratic rational for $i = 1, 2$, so by the inductive hypothesis we have that the primes dividing G/M_i are less or equal than 19 and distinct to 11, and the result follows in this case.

By last paragraph, let M be the unique minimal normal subgroup of G, which is elementary abelian. Since G/M is quadratic rational, by induction all prime divisors of $|G/M|$ satisfy the condition in the statement. Working by contradiction, we can assume that M is a p-group for a prime $p > 19$ or $p = 11$. In particular, p does not divide $|G/M|$.

Now, let H be a complement of M in G. Then $V = \mathrm{Irr}(M)$ is a $\mathbb{Z}_p[H]$-module, where the action of H is defined by conjugation. Also, since M is a minimal normal subgroup of G, we have that V is an irreducible module. Let F be an algebraic clousure of $\mathbb{Z}_p$, and suppose that $\mathcal{X}$ is a $\mathbb{Z}_p$-representation of G affording V. We write η for the Brauer character of H afforded by $\mathcal{X}^F$, as in Section 5.2.2.

Let $\varphi \in \mathrm{IBr}(H)$ be an irreducible constituent of η. Then by Theorem 5.10 we have that

$$\mathbb{Q}(\eta) \subseteq \mathbb{Q}(\varphi)\,.$$

Also, since p does not divide $|H|$, Theorem 5.6 implies that in fact $\varphi \in \mathrm{Irr}(H)$, and thus φ is either rational or quadratic, because $H \cong G/M$ is quadratic rational. In particular, we deduce that η is either rational or quadratic.

We claim that the action of H on V has the h-eigenvalue property, where $h = (p-1)/2$. Fix $\mu \in \mathbb{Z}_p^\times$ of order h, and let $\theta \in V$ be non-principal. Then $\mathbb{Q}(\theta) = \mathbb{Q}_p$, and so $\mathcal{G}_p = \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$ is cyclic of order $p-1$, by elementary Galois theory. Now, write T and T^* for the inertia and semi-inertia groups of θ in G, respectively. By Lemma 2.4, the equation $\theta^\sigma = \theta^g$ defines a group isomorphism $\rho : \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G)) \to T^*/T$, and Lemma 5.3 implies that the subgroup

$$\mathcal{H} = \mathrm{Gal}(\mathbb{Q}(\theta)/\mathbb{Q}(\theta^G)) = \rho^{-1}(T^*/T)$$

has index at most 2 in $\mathcal{G}_p$, since G is quadratic rational.

Now, let t be any integer coprime to p satisfying $t + p\mathbb{Z} = \mu \in \mathbb{Z}_p$, and recall that there exits a unique $\sigma_t \in \mathcal{G}_p$ such that $\xi^{\sigma_t} = \xi^t$, where $\xi \in \mathbb{C}$ is any primitive complex pth root of unity, by basic Galois theory (see Section 1.4). Then $o(\sigma_t) = o(\mu) = h$ and $\langle \sigma_t \rangle$ is the unique subgroup of order h of $\mathcal{G}_p$. Therefore $\langle \sigma_t \rangle \leq \mathcal{H}$, because $\mathcal{G}_p$ is cyclic, and there exists $g \in T^*$ such that $\theta^g = \theta^{\sigma_t}$. Since M is abelian, we have that $\theta^{\sigma_t}(x) = \theta(x^t) = \theta^t(x)$, for any $x \in M$, and therefore $\mu\theta = \theta^t = \theta^{\sigma_t}$, as desired.

By the claim, Theorem 5.11 applies to the action of H on V, so we have that $\mathbb{Q}(\eta)$ contains a primitive qth root of unity, for every prime $q \neq 3$ dividing $(p-1)/2$. Since $\mathbb{Q}(\eta)$ has degree at most 2 over $\mathbb{Q}$, this leads to $p - 1 = 2^a \cdot 3^b$, so in particular $p \neq 11$. Now if $p \leq 12\sqrt{3}$ then $p \leq 19$, and we are done in this case; otherwise, $a \leq 5$ and $b \leq 1$, and $a \leq 4$ if $b = 1$, by Theorem 5.11, again because $|\mathbb{Q}(\eta) : \mathbb{Q}| \leq 2$. This gives $p \leq 19$ in any case, and since $p \neq 11$, we obtain the desired contradiction. ∎

It is clear from last theorem that in order to complete the proof of Theorem D, we need to show that the order of a quadratic rational solvable group cannot be a multiple of 17 or 19, and we do so next. We mention that the proof of this fact contains arguments from Lemma 4.15 of [6] and Lemma 6 of [9].

Theorem 5.16. *Let G be a quadratic rational solvable group and p a prime divisor of $|G|$. Then $p \neq 17, 19$.*

Proof. We work by induction on $|G|$. Arguing as in the proof of Theorem 5.15, we can assume that G has a unique minimal normal subgroup M such that M is an elementary abelian p-group, for $p \in \{17, 19\}$, and p does not divide $|G/M|$.

Let H be a complement of M in G, so H acts on the $\mathbb{Z}_p$-vector space $V = \mathrm{Irr}(M)$ by conjugation, and the action has the h-eigenvalue property for $h = (p-1)/2$, by the same arguments as in the proof of Theorem 5.15. Since $G/M \cong H$ is quadratic rational, it follows from Theorem 5.10 that the character η of H afforded by V is either rational or quadratic.

Let $T \leq H$ be the stabilizer a non-trivial irreducible character of M in H, and choose T such that it is not properly contained in any other stabilizer in H of a non-trivial irreducible character of M. Let also $N = \mathbf{N}_H(T)$ and $W = \mathbf{C}_V(T)$. Then, by Lemma 5.14, the action of N/T on W is Frobenius, it has the h-eigenvalue property and if η_0 is the Brauer character of N/T afforded by W, then $\mathbb{Q}(\eta_0)$ is contained in $\mathbb{Q}(\eta)$. In particular, η_0 is either rational or quadratic.

By the previous paragraph, changing the notation if necessary, we can assume that H acts on V with the h-eigenvalue property, that this action is Frobenius, and that the character η of H afforded by V is either rational or quadratic. However, note that H does not need to be quadratic rational anymore. (Of course, we have identified $H = N/T$, $V = W$ and $\eta = \eta_0$, using the notation in the previous paragraph).

Assume first that $p = 19$, so the action of H on V has the 9-eigenvalue property. Here, we can argue as in Lemma 4.15 of [6]. Since $\mathbb{Q}(\eta)$ does not contain a primitive 9th root of unity, Lemma 5.13 applies, and we have that 3 divides the dimension of V. Write $\dim V = 3d$, and let L be the normal 3-complement of $\mathbf{O}^{3'}(G)$ (see the comments before Lemma 5.13). If L is cyclic, by Lemma 5.12 and Lemma 5.13, we have that $(2d+1)d \leq \Phi(|L|) \leq 6d$, which easily implies that $|L| \leq 42$. But by the cited results, we also have $|L| \geq (19^{2d} + 19^d + 1)/3 \geq 127$ and we get a contradiction. If L is not cyclic, then $q = 3$ and $\mathbf{O}_2(G) \cong Q_8$. Then $4d^2 \leq \Phi(|A|) \leq 6d$, where A is the normal cyclic 2-complement of L, by Lemma 5.12 and Lemma 5.13. This leads to $|A| \leq 18$, but by Lemma 5.13 we have that $|A| \geq (19^{2d} + 19^d + 1)/12 > 31$, a contradiction.

Assume now that $p = 17$ and that the Sylow 2-subgroups of G are cyclic. Arguing as before, since the action of H on V has the 8-eigenvalue property and $\mathbb{Q}(\eta)$ does not contain any primitive 8th root of unity, it follows by Lemma 5.13 that $\dim V = 2d$ for some integer d. As before, by Lemma 5.12 and Lemma 5.13 we have that $d(d+1)/2 \leq \Phi(|L|) \leq 4d$, where L is the normal cyclic 2-complement of $\mathrm{O}^{2'}(G)$ (see the comments before Lemma 5.13). This gives $|L| \leq 45$, and if $d = 1$ then $|L| \leq 5$. But by Lemma 5.13, $|L| \geq (17^d + 1)/2$, which is a contradiction.

Finally, suppose that $p = 17$ and that the Sylow 2-subgroups of G are generalized quaternion groups. Now, we can argue as in Step 5 of Lemma 6 of [9]. Let $S \in \mathrm{Syl}_2(G)$ and note that S has order at least 2^4, because the action of H in V has the 8-eigenvalue property and thus $\exp(S) \geq 8$. Let $\langle a \rangle$ be the unique cyclic maximal subgroup of S. The only normal subgroup of S of index 4 is $S' = \langle a^2 \rangle$. By Lemma 3.3 of [6], if $K = \mathrm{O}_2(H)$ then $|S : K|$ divides 4, and we deduce that $a^2 \in K$ (see comments before Lemma 5.13).

Let F be an algebraic closure of $\mathbb{Z}_p$. Let $\lambda \in F^\times$ be of order 8, and write $\lambda^2 = \sigma$. Then, for any $0 \neq v \in V$ there exists $h \in H$ of order 8 such that $v^h = \lambda v$. Since S contains a unique subgroup of order 8, we can assume that $h = a^{2^{t-3}}$, where $o(a) = 2^t \geq 2^3$. Hence $h^2 \in K$. Now, since $v^{h^2} = \sigma v$, notice that we have shown that for any non-zero $v \in V$ there exists $y \in K$ with $o(y) = 4$ such that $v^y = \sigma v$. Of course, the same conclusion is true if we change σ for σ^{-1} (to see this, just take $y^{-1} \in K$ instead of y).

Now, let $n \in H$ with $o(n) = 4$. Since the action of H on V is Frobenius and $F^\times$ has a unique cyclic subgroup of order 4, the eigenvalues of n on H are either σ or σ^{-1}. We can assume without loss that σ is an eigenvalue of n, so there exists a non-zero $v \in V$ such that $v^n = \sigma v$. Now, by the previous paragraph, there exists $y \in K$ such that $v^y = \sigma v$, and it follows by Frobenius action that $n = y$. In particular, K contains every element of order 4 of H, and we deduce that $K = S$, because the elements of order 4 of a generalized quaternion group generate the whole group.

By the previous paragraph, we have that H has a unique cyclic subgroup C of order 8. Then, by the previous 2 paragraphs, we have that every element n of H with $o(n) = 4$ is a power of an element of order 8 of C. In particular, every element of order 4 of H necessarily lies in C, which is a contradiction. ▌

In [6] it is proved that if G is a solvable group with $|\mathbb{Q}(G) : \mathbb{Q}| = n$ and p is a prime divisor of $|G|$, then $p \leq 16n^2 + 1$. Next we show that it is possible to bound the primes dividing $|G|$ just by looking at the fields of values of single irreducible characters of G. That is, if G is a solvable group satisfying the condition that $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ for all $\chi \in \mathrm{Irr}(G)$, then the set of prime divisors of $|G|$ is bounded in terms of k. Of course, this is Theorem E, which answers a question raised by A. Moretó and can used to give an alternative proof to Lemma 2.1 of [26].

Lemma 5.17. *Let k, n be positive integers. Suppose that $a_1, \ldots, a_s$ are distinct positive divisors of n satisfying $n/a_i \leq k$. Then $\mathrm{Gcd}\,(a_1, \ldots, a_s) \geq n(k-s)!/k!$.*

Proof. Write $\mathrm{Gcd}\,(a_1, \ldots, a_s) = (a_1, \ldots, a_s)$. Since the divisors a_i of n are distinct, we can assume that $n/a_i \leq k - i + 1$ for each i. We use induction on s.

Suppose first that $s = 2$. Then $n/(a_1, a_2) \leq (n/a_1)(n/a_2)$, and thus

$$(a_1, a_2) \geq n/(k(k-1)).$$

Suppose now that the inequality is true for any number of divisors a_i of n smaller than s. Since $(a_1, \ldots, a_s) = ((a_1, \ldots, a_{s-1}), a_s)$, we have that

$$n/(a_1, \ldots, a_s) \leq (n/(a_1, \ldots, a_{s-1}))(n/a_s) \leq k!/(k-s)!$$

by induction, and the result follows. ▌

Lemma 5.18. *Let G be a finite group satisfying that $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ for all $\chi \in \mathrm{Irr}(G)$. Suppose that $M \lhd G$ is p-elementary abelian for a prime p not dividing $|G : M|$. Then the natural action of G on $\mathrm{Irr}(M)$ has the h-eigenvalue property for some $h \geq (p-1)/k!$.*

Proof. Let $\theta \in \mathrm{Irr}(M)$ be non-principal, and write T, T^* for the inertia and semi-inertia groups of θ in G, respectively. By Lemma 5.3, T^*/T is isomorphic to a subgroup of index at most k of $\mathrm{Gal}(\mathbb{Q}_p/\mathbb{Q})$. Arguing as in the proof of Theorem 5.15, there exists $\mu \in \mathbb{Z}_p^\times$ with $o(\mu) \geq (p-1)/k$ and $g \in G$ such that $\theta^g = \mu\theta$.

Since there are at most k distinct positive divisors of $p-1$ which are greater or equal than $(p-1)/k$, it follows from Lemma 5.17 that

$$h = \mathrm{Gcd}\left\{o(\nu) \,|\, \nu \in \mathbb{Z}_p^\times,\ o(\nu) \geq (p-1)/k\right\} \geq (p-1)/k!\,.$$

Note that if $\lambda \in \mathbb{Z}_p^\times$ with $o(\lambda) = h$, then $\lambda \in \langle \mu \rangle$. In particular, since $\theta^g = \mu\theta$, we have that $\theta^{g^i} = \lambda\theta$ for some power g^i of g. We deduce that the action of G on $\mathrm{Irr}(M)$ has the h-eigenvalue property, as wanted. ∎

We shall need the following observation.

Lemma 5.19. *Let n be a positive integer, and assume that $n \neq 2, 6$. Write Φ for the Euler function. Then $n \leq \Phi(n)^2$.*

Proof. See Lemma 1.1 of [6]. ∎

Write $\pi(n)$ for the set of prime divisors of a positive natural number n.

Theorem 5.20. *There exists a function $f : \mathbb{N} \to \mathbb{N}$ such that for any solvable group G and any prime divisor p of $|G|$, if $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ for all $\chi \in \mathrm{Irr}(G)$ then $p \leq f(k)$.*

Proof. Define the function f by

$$f(m) = \max\left\{24m! + 1,\ m^2m! + 1\right\}.$$

We claim that $\pi(|G|)$ is bounded by $f(k)$. We use induction on $|G|$. Arguing as usual, we can assume that G has a unique minimal normal subgroup M. Of course, every $\chi \in \mathrm{Irr}(G/M)$ satisfies that $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$, and thus $\pi(|G/M|) \leq f(k)$ by induction. Also, M is an elementary abelian p-group, and we can assume that $p > f(k)$.

Let H be a complement of M in G, so $H \cong G/M$. By Lemma 5.18, the natural action of G on $\mathrm{Irr}(M)$ by conjugation has the h-eigenvalue property, for some integer $h \geq (p-1)/k!$. Let η be the Brauer character of H afforded by the $\mathbb{Z}_p$-module $\mathrm{Irr}(M)$. Then, by Theorem 5.11 we have that either $|\mathbb{Q}(\eta) : \mathbb{Q}| \geq p/(6\sqrt{3})$ or $\mathbb{Q}(\eta)$ contains a primitive $(h/(h,4))$th root of unity.

Suppose that $\varphi \in \mathrm{IBr}(H)$ is a constituent of η. Then, by Theorem 5.10, we have that $\mathbb{Q}(\eta)$ is contained in $\mathbb{Q}(\varphi)$. We can view φ as a character of G/M. Note that since p does not divide $|G/M|$ we have that $\varphi \in \mathrm{Irr}(G/M)$, and thus $|\mathbb{Q}(\varphi) : \mathbb{Q}| \leq k$ by hypothesis. In particular, $|\mathbb{Q}(\eta) : \mathbb{Q}| \leq k$.

By assumption, we have that $p > f(k) > 6\sqrt{3}k$, and hence $\mathbb{Q}(\eta)$ contains a primitive $(h/(h,4))$th root of unity, by Theorem 5.11. In particular $|\mathbb{Q}(\eta) : \mathbb{Q}| \geq \Phi(h/(h,4))$,

where Φ is the Euler function. Observe that if $h/(h,4) \in \{2,6\}$ then $h \leq 24$ and thus $p \leq 24k! + 1 \leq f(k)$. So $h/(h,4) \neq 2,6$ and then

$$h \leq h/(h,4) \leq \Phi(h/(h,4))^2,$$

by Lemma 5.19. But this implies that $p \leq k^2k! + 1 \leq f(k)$, a contradiction. ▮

5.4 Some related results

Our main purpose in this section is to give a positive answer to Problem 1 of [3]. More precisely, we prove that there is a number which is an upper bound for the degree $|\mathbb{Q}(G) : \mathbb{Q}|$, where G is any solvable semi-rational group. We shall appeal to the following elementary number-theoretic lemma. Recall that an algebraic complex number ω is quadratic over the rationals if $|\mathbb{Q}(\omega) : \mathbb{Q}| = 2$.

Lemma 5.21. *Let L be a subfield of $\mathbb{C}$. Then L is generated over $\mathbb{Q}$ by quadratic elements if and only if $L/\mathbb{Q}$ is a Galois extension and $\mathrm{Gal}(L/\mathbb{Q})$ is an elementary abelian 2-group.*

Proof. See Lemma 8 of [3]. ▮

Theorem 5.22. *Let G be a solvable semi-rational group. Then $|\mathbb{Q}(G) : \mathbb{Q}| \leq 2^7$.*

Proof. Write $|G| = n$. Of couse, we can assume that G is not a rational group. By Lemma 5.2, the field $\mathbb{Q}(G)$ is generated by quadratic elements over $\mathbb{Q}$, and of course $\mathbb{Q}(G) \subseteq \mathbb{Q}_n$. By the previous lemma we have that $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}(G)/\mathbb{Q})$ is an elementary abelian 2-group.

Write $\mathcal{G}_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. Now $\mathcal{G} \cong \mathcal{G}_n/\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(G))$, and thus $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}(G))$ contains the normal 2-complement of $\mathcal{G}_n$. Then $\mathcal{G}$ is isomorphic to an elementary abelian factor group of the Sylow 2-subgroup $\mathcal{P}$ of $\mathcal{G}_n$.

For any prime divisor p of $|G|$, write $\mathcal{G}_p$ for the Galois group of $\mathbb{Q}_{|G|_p}$ over $\mathbb{Q}$. Note that $\mathcal{G}_2$ is an abelian 2-group of rank at most 2, and the Sylow 2-subgroup of $\mathcal{G}_p$ is cyclic for any odd prime p. Since $\mathcal{G}_n \cong \mathcal{G}_{p_1} \times \cdots \times \mathcal{G}_{p_l}$, where $p_1, \ldots, p_l$ are the distinct prime divisors of $|G|$, in any case it follows that $\mathcal{P}$ can be generated by $l+1$ elements. Hence $|\mathcal{P}/\Phi(\mathcal{P})| \leq 2^{l+1}$, and we deduce that $|\mathbb{Q}(G) : \mathbb{Q}| \leq 2^{l+1}$. Now, since G is semi-rational, its order $|G|$ is divisible by at most 6 distinct primes, by Theorem 5.1, and so we obtain the bound $|\mathbb{Q}(G) : \mathbb{Q}| \leq 2^7$, as wanted. ▮

Note that the arguments in the previous proof also apply to a quadratic rational solvable group G, because $\mathrm{Gal}(\mathbb{Q}(G)/\mathbb{Q})$ is elementary abelian, by Lemma 5.21. Hence, we can use Theorem D to obtain an analogue of the last theorem.

Proposition 5.23. *Let G be a quadratic rational solvable group. If $|G|$ is divisible by l distinct primes, then $|\mathbb{Q}(G) : \mathbb{Q}| \leq 2^{l+1}$. In particular, $|\mathbb{Q}(G) : \mathbb{Q}| \leq 2^6$.*

It is clear that the field $\mathbb{Q}(G)$ generated by the values of all irreducible characters of a group G is the smallest field containig all the fields $\mathbb{Q}(\chi_1), \ldots, \mathbb{Q}(\chi_s)$, where $\chi_1, \ldots, \chi_s$ are the irreducible characters of G. In a similar fashion as before, we have the following more general result.

Theorem 5.24. *There exists a function $d : \mathbb{N} \to \mathbb{N}$ such that for any solvable group G and any prime divisor p of $|G|$, if $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ for all $\chi \in \mathrm{Irr}(G)$ then $|\mathbb{Q}(G) : \mathbb{Q}| \leq d(k)$.*

Proof. By Theorem E, the set $\pi(|G|)$ is bounded in terms of k. Hence, if $p_1, \ldots, p_l$ are the prime divisors of $|G|$, then l is bounded in terms of k.

Of course, $\mathbb{Q}(G)$ is contained in $\mathbb{Q}_{|G|}$. Since $|\mathbb{Q}(\chi) : \mathbb{Q}| \leq k$ for every $\chi \in \mathrm{Irr}(G)$, it suffices to show that the number of field extensions $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}_{|G|}$ with $|L : \mathbb{Q}| \leq k$ is bounded in terms of k. By basic Galois theory, this is equivalent to show that the number of subgroups $\mathcal{H}$ of $\mathcal{G} = \mathrm{Gal}(\mathbb{Q}_{|G|}/\mathbb{Q})$ with $|\mathcal{G} : \mathcal{H}| \leq k$ is bounded in terms of k. Since $\mathcal{G}$ is abelian, this is the same as proving that the number of subgroups $\mathcal{H} \leq \mathcal{G}$ of order $|\mathcal{H}| \leq k$ is bounded by a function of k.

By last paragraph, it is clear that the result will follow if we prove that the number of elements in $\mathcal{G}$ of order less or equal than k is bounded in terms of k. Now, for each prime divisor p of $|G|$, write $\mathcal{G}_p = \mathrm{Gal}(\mathbb{Q}_{|G|_p}/\mathbb{Q})$, and note that $\mathcal{G} = \mathcal{G}_{p_1} \times \cdots \times \mathcal{G}_{p_l}$. Observe that it suffices to show that for each $1 \leq i \leq l$, the number of elements of order at most k in $\mathcal{G}_{p_i}$ is bounded in terms of k, because l is bounded in terms of k. This is clear when p_i is odd because $\mathcal{G}_{p_i}$ is cyclic. Since $\mathcal{G}_2$ is an abelian group of rank at most 2, an elementary argument yields to the same conclusion in this case. ∎

5.5 Examples

As mentioned in the introduction of the chapter, if p is a prime in $\{2, 3, 5, 7, 13\}$, then the Frobenius group of order $p(p-1)/2$ is quadratic rational, so no prime can be removed from the list given in Theorem D.

Let G be a group of odd order. By G. Navarro's Theorem A of [28], the number of irreducible quadratic characters of G equals the number of quadratic conjugacy classes of G. In particular, since the only rational class of G is the class containing the identity and the unique irreducible rational character of G is the principal character (because G has odd order), it follows that G is quadratic rational if and only if G is semi-rational, when $|G|$ is odd. As a consequence, a quadratic rational group of odd order is either a 3-group or a $\{3, 7\}$-group and its structure is known (see Theorem 3 of [3]).

It is not true that the families of quadratic rational groups and semi-rational groups coincide, even if we restrict ourselves to solvable groups. For instance, the group G of order 32 defined by

$$G = \langle a, b, c \,|\, a^2 = b^2 = c^8 = 1,\ [b, c] = 1,\ b^a = bc^4,\ c^a = c^3 \rangle,$$

is semi-rational but it is not quadratic rational. Similarly, the group

$$H = \langle a, b, c \,|\, a^2 = b^2 = c^8 = 1,\ [a, b] = 1,\ [b, c] = 1,\ c^a = bc^3 \rangle,$$

which also has order 32, is quadratic rational but it is not semi-rational. (In particular, note that the natural actions of $\mathrm{Gal}(\mathbb{Q}_{32}/\mathbb{Q})$ on the set of irreducible characters of G and on the set of conjugacy classes of G are not permutation isomorphic, and the same holds for H. In fact, G and H are groups of smallest possible order satisfying this.)

Finally, we construct some examples of quadratic rational solvable groups of order divisible by 13. Let $\mathbb{F}$ be the field of 13 elements and suppose that $\langle \xi \rangle = \mathbb{F}^\times$. Write

$G = \mathrm{GL}(2,13)$, and let $P \in \mathrm{Syl}_{13}(G)$ be generated by $a = \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}$. Note that both elements

$$b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and

$$c = \begin{pmatrix} \xi^2 & 0 \\ 0 & \xi^4 \end{pmatrix}$$

of G normalize P. Now, the subgroup $\langle a, b, c \rangle = H \leq G$ has order $|H| = 2^2 \cdot 3 \cdot 13$ and is quadratic rational. Furthermore, the semidirect product $V \rtimes H$ of H with the natural module $V = V(2,13)$ is quadratic rational. Also, if

$$I = \langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \xi & 0 \\ 0 & -\xi \end{pmatrix} \rangle \leq G$$

then $V \rtimes I$ has order $2^3 \cdot 3 \cdot 13^2$ and is quadratic rational.

Bibliography

[1] Y. Berkovich, Z. Janko, Groups of prime power order, Vol. 2, Walter de Gruyter, Berlin, 2008.

[2] A. M. Broshi, Galois correspondences between the irreducible characters and the conjugacy classes of finite groups, J. Algebra **19** (1971), 441–451.

[3] D. Chillag, S. Dolfi, Semi-rational solvable groups, J. Group Theory **13** (2010), no. 4, 535–548.

[4] P. Centella, G. Navarro, Correspondences between constituents of projective characters, Arch. Math. (Basel) **90** (2008), 289–294.

[5] E. C. Dade, Galois Actions on characters and on classes, privately circulated.

[6] E. Farias e Soares, Big primes and character values for solvable groups, J. Algebra **100** (1986), 305–324.

[7] W. Feit, G. Seitz, On finite rational groups and related topics, Illinois J. Math. **33** (1998), no. 1, 103–131.

[8] The GAP Group, GAP Groups, Algorithms and Programming, Version 4.4.12, 2008 (http://www.gap-system.org).

[9] R. Gow, Groups whose characters are rational-valued, J. Algebra **40** (1976), no. 1, 280–299.

[10] J. S. Graves, Glauberman-Isaacs correspondence and π-Brauer characters, J. Algebra **169** (1994), no. 3, 891–901.

[11] P. Hall, G. Higman, On the p-length of p-soluble groups and reduction theorems for Burnside's problem, Proc. London Math. Soc. (3) **6** (1956).

[12] B. Huppert, N. Blackburn, Finite Groups II, Springer-Verlag, Berlin et al., 1982.

[13] M. Isaacs, Character Theory of Finite Groups, AMS Chelsea Publishing, Providence, R. I., 2006.

[14] M. Isaacs, Finite Group Theory, American Mathematical Society, Providence, R. I., 2008.

[15] M. Isaacs, Characters and Hall subgroups of groups of odd order, J. Algebra **157** (1993), 548–561.

[16] M. Isaacs, Characters of π-separable groups, J. Algebra **86** (1984), 98–128.

[17] M. Isaacs, Characters of solvable and symplectic groups, Amer. J. Math. **95** (1973), no. 3, 594–635.

[18] M. Isaacs, G. Navarro, Solvable groups having only three rational classes of 2-elements, to appear in Arch. Math. (Basel).

[19] M. Isaacs, G. Navarro, Sylow 2-subgroups of rational groups, to appear in Math. Z.

[20] M. Isaacs, G. Navarro, J. Sangroniz, p-Groups with few almost-rational conjugacy classes, Israel J. Math., DOI: 10.1007/s11856-011-0153-y.

[21] M. Isaacs, G. Navarro, L. Sanus, Field of values of Fong characters, Arch. Math. (Basel) **86** (2006), 305–309.

[22] N. Jacobson, Basic Algebra I, W. H. Freeman and Co., San Francisco, 1974.

[23] Z. Janko, A classification of finite 2-groups with exactly three involutions, J. Algebra **291** (2005), 505–533.

[24] H. Kurzweil, B. Stellmacher, The theory of finite groups, Springer-Verlag, New York, 2004.

[25] S. Mattarei, On character tables of wreath products, J. Algebra **175** (1995), 157–178.

[26] A. Moretó, Complex group algebras of finite groups: Brauer's problem 1, Adv. Math. **208** (2007), no. 1, 236–248.

[27] G. Navarro, Characters and blocks of finite groups, Cambridge University Press, Cambridge, 1998.

[28] G. Navarro, Quadratic characters in groups of odd order, J. Algebra **322** (2009), no. 7, 2586–2589.

[29] G. Navarro, Fields, values and character extensions in finite groups, J. Group Theory **10** (2007), 279–285.

[30] G. Navarro, J. Tent, Rationality and Sylow 2-subgroups, Proc. Edinb. Math. Soc. (2) **53** (2010), no. 3, 787–798.

[31] G. Navarro, P. H. Tiep, Rational irreducible characters and rational conjugacy classes in finite groups, Trans. Amer. Math. Soc. **360** (2008), no. 5, 2443–2465.

[32] J. Sangroniz, J. Tent, 2-groups with few rational conjugacy classes, J. Algebra, **338**, no. 1, (2011), 114–121.

[33] J. Tent, p-Length and p'-degree irreducible characters having values in $\mathbb{Q}_p$, submitted.

[34] J. Tent, 2-Length and rational characters of odd degree, Arch. Math. (Basel) **96** (2011), no. 3, 201–206.

[35] J. Tent, Quadratic rational solvable groups, submitted.

[36] J. G. Thompson, Composition factors of rational finite groups, J. Algebra **319** (2008), no. 2, 558–594.

[37] T. Wilde, The real part of the character table of a finite group, Comm. Algebra **35** (2007), no. 12, 4042–4056.

[38] T. R. Wolf, Character correspondences and π-special characters in π-separable groups, Canad. J. Math. **39** (1987), no. 4, 920–937.

UNIVERSITAT DE VALÈNCIA
FACULTAT DE MATEMÀTIQUES

reunido el tribunal que suscribe, en el dia de la fecha, acordó otorgar a esta Tesis Doctoral de D. Joan F. Tent i Forgas

la calificación de Sobresaliente Cum Laude

Valencia, a 1 de Juno 2012

El Presidente/a, El Secretario/a,